Computing abstractions of nonlinear systems

Gunther Reißig*

Abstract

Sufficiently accurate finite state models, also called symbolic models or discrete abstractions, allow one to apply fully automated methods, originally developed for purely discrete systems, to formally reason about continuous and hybrid systems, and to design finite state controllers that provably enforce predefined specifications. We present a novel algorithm to compute such finite state models for nonlinear discrete-time and sampled systems which depends on quantizing the state space using polyhedral cells, embedding these cells into suitable supersets whose attainable sets are convex, and over-approximating attainable sets by intersections of supporting half-spaces. We prove a novel recursive description of these half-spaces and propose an iterative procedure to compute them efficiently. We also provide new sufficient conditions for the convexity of attainable sets which imply the existence of the aforementioned embeddings of quantizer cells. Our method yields highly accurate abstractions and applies to nonlinear systems under mild assumptions, which reduce to sufficient smoothness in the case of sampled systems. Its practicability in the design of discrete controllers for nonlinear continuous plants under state and control constraints is demonstrated by an example.

Index Terms

Discrete abstraction, symbolic model, nonlinear system, symbolic control, motion planning, formal verification, polyhedral over-approximation, attainability, attainable set; MSC: Primary, 93C10; Secondary, 93C55, 93C57, 93C15, 93B03

I. Introduction

In recent years, there has been a growing interest in using finite state models for the analysis and synthesis of continuous and hybrid systems [1]–[9]. This interest has been stimulated by safety critical applications [10], inherent limits of continuous feedback control [11, Sections 5.8-5.10], increasingly complex control objectives [12], and the necessity to cope with the effects of coarse quantization [13]. A sufficiently accurate finite state model, also called a *symbolic model* or *discrete abstraction*, would allow one to apply fully automated methods, originally developed for purely discrete systems [14]–[16], to formally reason about the original system, and to design finite state controllers that provably enforce predefined specifications [2]–[9]. Obtaining such abstractions constitutes a challenging problem, which has only been satisfactorily solved for special cases.

Under the name *symbolic dynamics*, finite state models of continuous systems had already been a well-established mathematical tool [17] when the concept appeared in the engineering literature [18], [19]. Much of the subsequent research has been devoted to systems whose continuous-valued dynamics is linear. Methods for nonlinear systems have been systematically studied since around 1980; see [1], [4]–[9]. In the earliest

*Universität Kassel, Fachbereich 16 - Elektrotechnik/Informatik, Regelungs- und Systemtheorie, Wilhelmshöher Allee 73, D-34121 Kassel, Germany, http://www.reiszig.de/gunther/

This work has been accepted for publication in the *IEEE Trans. Automatic Control*. Copyright may be transferred without notice, after which this version may no longer be accessible. Please refer to author's homepage and to IEEE Xplore for the definite publication. You may also find a BibTEX entry at the former website.

such approach [20], attainable sets are approximated by means of trajectories emanating from a finite set of initial points, hence the name *sampling method* [20]. This method has been successfully applied to a variety of problems [1], [4]–[8], [21]–[23], including symbolic control of sampled systems [23], [24]. An extension allows for rigorous over-approximation of attainable sets [25], and thus, for the computation of abstractions. Over the years, a large number of alternatives to the sampling method have been proposed, which represent a variety of compromises between approximation accuracy, practicability, rigor, and computational complexity [23], [26]–[42].

In the present paper, we aim at computing abstractions for nonlinear discrete-time systems of the form

$$x_{k+1} = G(x_k, u_k), \tag{1}$$

where the state x takes values in a subset of $\mathbb{R}^n$, and u is an input signal which is assumed to take its values in some finite set U. If (1) arises from a continuous-time system

$$\dot{x} = F(x, v) \tag{2}$$

under sampling, its right hand side G may not be explicitly given. Our results will still apply as we will formulate hypotheses to be verified and computations to be performed directly in terms of the right hand side F of (2).

The approach we follow involves quantizing the state space of (1) with the help of a finite covering C of $\mathbb{R}^n$ whose elements we call *cells* [1]–[9]. The system (1) is supplemented with a *quantizer* Q which assigns to any state x of (1) the collection of those cells in C that contain x, $Q(x) = \{\Delta \in C \,|\, x \in \Delta\}$. That is, a pair (u, Δ) of an input signal $u_0, u_1, \ldots$ and an output signal $\Delta_0, \Delta_1, \ldots$ could possibly be generated by the *quantized system* composed of (1) and the non-deterministic output relation

$$\Delta_k \in Q(x_k) \tag{3}$$

iff there exists a sequence $x_0, x_1, \ldots$ such that (1) and (3) hold for all non-negative integers k[1]. The collection of such pairs (u, Δ) is called the *behavior* of the quantized system (1),(3) [43].

The input alphabet U and the output alphabet C of the quantized system (1),(3) are both finite. Control problems for (1),(3) can still be challenging to solve, especially if the system (1) is nonlinear and the specification involves constraints or is otherwise complex. In contrast, controllers (or *supervisors*) for finite automata are generally straightforward to design [14], [16], which raises the question of whether controllers for the quantized system (1),(3) can be obtained by solving auxiliary control problems for automata that approximate the behavior of (1),(3). As it turns out, this strategy is feasible if the approximation is both conservative and sufficiently precise, e.g. [3], [44]–[46]. That is, the automaton must be capable of generating any signal in the behavior of (1),(3), and the set of spurious signals should be small. In other words, the said strategy requires a *discrete abstraction*, by which we mean a superset of the behavior of (1),(3) that can be realized by a finite automaton, and this abstraction should be as accurate as possible.

One way to prescribe the accuracy of an abstraction is to restrict the extent by which its signals are allowed to violate the dynamics of (1),(3). While, by definition, signals in the behavior of the quantized system (1),(3) are consistent with the dynamics of (1),(3) at all times, a common class of abstractions require consistency only on finite

[1] The symbols u, x and Δ are used to denote elements of U, $\mathbb{R}^n$ and C, respectively, as well as signals taking their values in these sets.

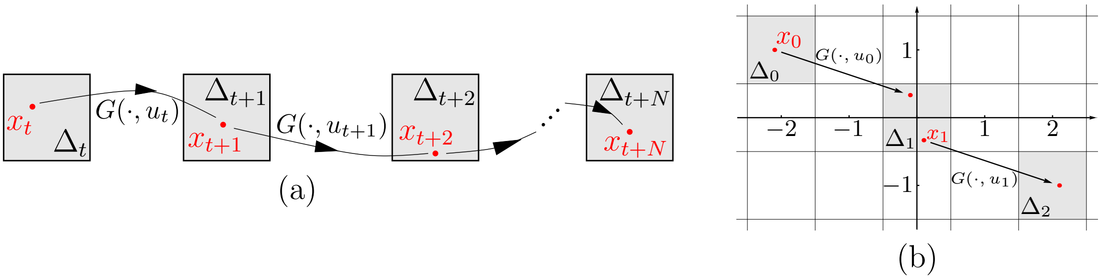


Figure 1. (a) Illustration of consistency with the dynamics of the quantized system (1),(3) on finite time intervals. (b) Quantizer cells may serve as states of automata realizations of abstractions of memory span 1, where transitions are defined by condition (4).

time intervals [44], [45]. Such an abstraction contains any pair (u, Δ) that fulfills the following condition, in which the *memory span* $N \geq 1$ determines the accuracy [43]: For any non-negative integer t there are states $x_t, \dots, x_{t+N}$ such that (1) and (3) hold for all $k \in \{t, t+1, \dots, t+N-1\}$ and $k \in \{t, t+1, \dots, t+N\}$, respectively. See Fig. 1(a).

In the case that $N = 1$, consistency of (u, Δ) is equivalent to the existence of a sequence $x_0, x_1, \dots$ for which

$$x_k \in \Delta_k \quad \text{and} \quad G(x_k, u_k) \in \Delta_{k+1} \tag{4}$$

hold for all k. Hence, the cells in the covering C may serve as states of an automaton realization of the abstraction, where the occurrence of an input symbol $u_k \in U$ enables a transition from $\Delta_k \in C$ to $\Delta_{k+1} \in C$ iff there is a state x_k of (1) such that (4) holds. Obviously, that automaton will be capable of generating any pair of signals u and Δ in the behavior of (1),(3). The fact that it will generally also generate spurious signals is illustrated in Fig. 1(b). If (1) requires the sign of the second component of the state to be constant, then the sequence $\Delta_0, \Delta_1, \Delta_2, \dots$ of cells generated by the automaton is not consistent with the dynamics of (1),(3). In contrast, consistency of (u, Δ) for $N > 1$ requires, amongst other conditions, that (4) holds with $x_1 = G(x_0, u_0)$, which rules out the spurious signal $\Delta_0, \Delta_1, \Delta_2, \dots$ of Fig. 1(b). Indeed, increasing the memory span N generally results in more accurate abstractions.

In this paper we shall present a novel algorithm to compute abstractions of finite but otherwise arbitrary memory span that builds on a well-known reformulation of consistency on finite time intervals in terms of attainable sets [44], [45], on a new method to compute polyhedral over-approximations of the latter, and on new results that guarantee the convexity of attainable sets of (1) and (2).

In our approach, polyhedral quantizer cells are embedded into suitable supersets whose attainable sets under the dynamics of (1) are convex for the duration of N time steps, where N is the memory span of the abstraction that is being computed. That convexity requirement permits us to over-approximate attainable sets by intersections of supporting half-spaces, and the latter are obtained from systems of linear equations derived from (1). The number of half-spaces needed can be quite large, especially if the memory span exceeds 1. We present a novel recursive description of these half-spaces and propose an iterative procedure to compute them efficiently.

The existence of the aforementioned embeddings of quantizer cells is, in fact, the essential requirement for our method to apply. The results in this paper not only allow verification of that requirement when a particular quantizer is given, but they also show how to meet it using sufficiently small but otherwise arbitrary polyhedral cells. We use strongly convex supersets of quantizer cells, and the error by which we over-approximate attainable sets depends quadratically on the size of the cells. Application of our earlier results [47], [48] on ellipsoidal supersets would have led to linear error bounds. Thus, the accuracy of the computed abstractions is improved if a particular quantizer is given. Alternatively, fewer and larger cells may be used, which reduces the computational effort to compute abstractions and also reduces the complexity of controllers designed on the basis of the latter. These results are obtained under mild assumptions on the right hand side G of (1), which reduce to sufficient smoothness in the case of sampled systems.

The remaining of this paper is organized as follows. The next section introduces basic notation and terminology. In Section III we present our algorithm for the computation of abstractions, prove its correctness, and analyze its computational complexity. Section IV is devoted to our results on the convexity of attainable sets. In Section V, practicability of our approach in the design of discrete controllers for nonlinear continuous plants under state and control constraints is demonstrated by an example. We also present computational results on how the computational effort of our approach grows with the problem size.

II. Preliminaries

A. Basic notation

$\mathbb{R}$ and $\mathbb{Z}$ denote the sets of real numbers and integers, respectively, $\mathbb{R}_+$ and $\mathbb{Z}_+$, their subsets of non-negative elements, and $\mathbb{N} = \mathbb{Z}_+ \setminus \{0\}$. $[a, b]$, $]a, b[$, $[a, b[$, and $]a, b]$ denote closed, open and half-open, respectively, intervals with end points a and b, e.g. $[0, \infty[= \mathbb{R}_+$. $[a; b]$, $]a; b[$, $[a; b[$, and $]a; b]$ stand for discrete intervals, e.g. $[a; b] = [a, b] \cap \mathbb{Z}$.

For any sets A and B, $f \colon A \to B$ denotes a map of A into B, and B^A is the set of all such maps. Operations involving subsets of $\mathbb{R}^n$ are defined pointwise [49, Appendix A], e.g. $\Delta + \Delta' := \{\omega + \omega' \,|\, \omega \in \Delta, \omega' \in \Delta'\}$ and $\varphi([0, t], \Delta) := \{\varphi(\tau, \omega) \,|\, \tau \in [0, t], \omega \in \Delta\}$ if $\Delta, \Delta' \subseteq \mathbb{R}^n$, $\varphi \colon \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$, and $t \in \mathbb{R}$.

C^k denotes the class of k times continuously differentiable maps, and $C^{k,1}$, the class of maps in C^k with (locally) Lipschitz-continuous kth derivative.

B. Behaviors

Given an arbitrary set W called *signal alphabet*, any subset $B \subseteq W^{\mathbb{Z}_+}$ is a *behavior* on W [43]–[46], [50]. Hence, elements of B are infinite sequences $w \colon \mathbb{Z}_+ \to W$, which we call *signals*. We denote the value of the signal w at time k by w_k. The *backward τ-shift* σ^τ is defined by $(\sigma^\tau w)_k = w_{\tau+k}$. The *restriction* of B to $I \subseteq \mathbb{Z}_+$, $B|_I$, is defined by $B|_I := \{w|_I \,|\, w \in B\}$. B is *time-invariant* if $\sigma^1 B \subseteq B$. B is *N-complete*, or equivalently, B has *memory span* N, if $N \in \mathbb{Z}_+$ and $B = \left\{ w \in W^{\mathbb{Z}_+} \,\middle|\, \forall_{\tau \in \mathbb{Z}_+} \, (\sigma^\tau w)|_{[0;N]} \in B|_{[0;N]} \right\}$. A superset B' of a behavior $B \subseteq W^{\mathbb{Z}_+}$ is called an *abstraction* of B, and B' is additionally called *discrete* if it can be realized by a finite automaton.

C. Discrete-time systems

In (1) with right hand side $G \colon X \times U \to X$, $u \colon \mathbb{Z}_+ \to U$ represents an input signal and $x \colon \mathbb{Z}_+ \to X$, a state signal. A *trajectory* of (1) is a sequence $(x, u) \colon \mathbb{Z}_+ \to X \times U$ for which (1) holds for all $k \in \mathbb{Z}_+$. The collection of such trajectories, which is a subset of $(X \times U)^{\mathbb{Z}_+}$, is called the *behavior* of (1). The *general solution* $\psi \colon \mathbb{Z}_+ \times X \times U^{\mathbb{Z}_+} \to X$ of (1) is the map defined by the requirement that $(\psi(\cdot, x_0, u), u)$ is a trajectory of (1) and

$\psi(0, x_0, u) = x_0$. Of course, it is not necessary to specify u on the whole time axis, so we may write

$$\psi(k, x_0, u_0, \dots, u_{k'-1}) := \psi(k, x_0, u|_{[0,k'[}) := \psi(k, x_0, u)$$

whenever $k' \geq k$. We will often assume the following.

($\mathbf{H_1}$) $X \subseteq \mathbb{R}^n$ is open and $G\colon X \times U \to X$ is such that for all $u \in U$, the map $G(\cdot, u)$ is a C^1-diffeomorphism onto an open subset of X.

We will say *(H_1) is fulfilled with smoothness C^K* if (H_1) holds with $G(\cdot, u)$ of class C^K rather than merely C^1.

III. Computation of abstractions

In the present section, we shall develop an efficient algorithm for computing abstractions of (1) that can be represented by finite automata. Intuitively, our approach is that of successively expanding the behavior of (1) and may be seen to comprise four approximation steps: State space quantization, approximation by the smallest discrete abstraction, approximation by a collection of convex programs, approximation by a collection of linear programs.

The purpose of state space quantization is to conservatively approximate (1) using a finite signal alphabet, which is an important prerequisite for a finite automaton approximation. Unfortunately, 1-completeness of the behavior of (1) is usually lost, and in general the behavior of the quantized system is not N-complete for any N. In order to reintroduce N-completeness, which is sufficient for a finite automaton representation to exist, we approximate the quantized system again, this time by the smallest discrete abstraction of memory span N. A problem with the latter abstraction is that it may only be computed exactly for special cases of both systems (1) and state space quantizations. Two more approximation steps yield further abstractions, which are both N-complete and characterized in terms of computationally tractable problems. Specifically, we first replace each quantizer cell by a suitable superset whose attainable sets are known to be convex, and then determine tight polyhedral over-approximations, i.e., collections of supporting half-spaces, of the latter. This yields abstractions characterized in terms of linear programs. As it turns out, each half-space can be obtained as a solution of a system of linear equations derived from (1) and of differential equations derived from (2), respectively.

A. State space quantization

Quantization of the state space of (1) is realized by supplementing (1) with a quantizer; see Section I.

The system C of quantizer cells is chosen as follows. We first define a region K of the state space X of (1) whose local dynamics is deemed an essential part of the behavior of (1), then choose a finite covering C' of K, and finally supplement C' by additional cells in order to obtain a covering C of $\mathbb{R}^n$. Intuitively, K is the intended operating range of the quantizer, whereas cells in $C \setminus C'$ represent overflow symbols.

Of course, what is considered essential local dynamics depends on the purpose of our analysis of (1), and our choice of C' will also be influenced by other particularities of the problem at hand; hence a general rule for the choice of the quantizer cannot be given. However, the following hypothesis should be fulfilled in order to ensure the correctness of the algorithm for the computation of abstractions we are going to present.

($\mathbf{H_2}$) The input alphabet U is finite, and C is a finite covering of $\mathbb{R}^n$ whose elements are nonempty convex polyhedra. For each cell $\Delta \in C' \subseteq C$ there is a superset, denoted $\widehat{\Delta}$ in the sequel, for which $\widehat{\Delta} \subseteq X$ and attainable sets $\psi(k, \widehat{\Delta}, u)$ are convex for all $k \in [1; N]$ and all $u \colon [0; k[\to U$, where ψ denotes the general solution of (1), and N, the memory span of the abstraction we seek to obtain.

In the present section, the above condition plays the role of an assumption. The nontrivial question of how to verify it is postponed to Section IV.

B. Smallest discrete abstractions

Let $B \subseteq (U \times C)^{\mathbb{Z}_+}$ denote the behavior of the quantized system (1),(3), and let $N \in \mathbb{Z}_+$ be given. The *N-complete hull* B_N of B is the intersection of all N-complete behaviors $B' \subseteq (U \times C)^{\mathbb{Z}_+}$ that contain B as a subset. Under the name *strongest N-complete approximations*, N-complete hulls have been introduced and investigated by Moor and his collaborators, e.g. [44], [45]. It has been shown that $B \subseteq B_{N+1} \subseteq B_N$ and that N-complete hulls are indeed N-complete.Thus, the map that assigns to B its N-complete hull B_N is a closure operator [51], and B_N is the smallest discrete abstraction of memory span N of B. Moreover, B_N admits the following characterization [44], [45].

III.1 Proposition. *Let C be a covering of $\mathbb{R}^n$, $N \in \mathbb{Z}_+$, $u \colon [0; N] \to U$, $\Delta \colon [0; N] \to C$, ψ the general solution of (1), B the behavior of the quantized system (1),(3), and B_N the N-complete hull of B. Then*

$$B_N = \left\{ w \colon \mathbb{Z}_+ \to W \,\middle|\, \forall_{\tau \in \mathbb{Z}_+} \, (\sigma^\tau w)|_{[0;N]} \in B|_{[0;N]} \right\}.$$

Moreover, the sets $M_0, \ldots, M_N$ defined by

$$M_k = \left\{ \psi(k, x_0, u) \,\middle|\, x_0 \in X, \forall_{\tau \in [0;k]} \, \psi(\tau, x_0, u) \in \Delta_\tau \right\} \tag{5}$$

satisfy $M_k = \Delta_k \cap G(M_{k-1}, u_{k-1})$ for all $k \in [1; N]$, and for all $k \in [0; N]$ we have $(u, \Delta) \in B|_{[0;k]}$ iff $M_k \neq \emptyset$.

In view of Proposition III.1, computing an exact representation of the k-complete hull B_k of the behavior of (1),(3) would require verifying

$$M_k(u, \Delta) \neq \emptyset \tag{6}$$

for all choices of sequences u and Δ, where $M_k(u, \Delta)$ is defined by the right hand side of (5). To verify (6), in turn, one must check whether there is some initial point $x_0 \in \Delta_0$ such that the trajectory generated by x_0 and u visits $\Delta_1, \ldots, \Delta_k$ at times $1, \ldots, k$; see also Fig. 1(a). (In fact, $M_k(u, \Delta)$ consists of the values at time k of the trajectories that satisfy the latter condition.) To perform that test is, in general, an extremely difficult problem which may only be exactly solved in rather special situations. One therefore aims at efficiently computing discrete abstractions that conservatively approximate the smallest one, B_k, and resort to a test

$$\widehat{M_k}(u, \Delta) \neq \emptyset \tag{7}$$

for some outer approximation $\widehat{M_k}(u, \Delta)$ of $M_k(u, \Delta)$, e.g. [28]. On the one hand, the set $\widehat{M}(u, \Delta)$ should have a simple structure in order to allow for efficiently testing condition (7). On the other hand, that set should approximate $M(u, \Delta)$ as accurately as possible, since B_k already is an over-approximation of the actual behavior of the quantized system

(1),(3) and the difference $\widehat{M}(u,\Delta) \setminus M(u,\Delta)$ will inevitably lead to additional spurious signals.

The following novel characterization of B_k, which is not valid in the more general setting of [44], [45], will be crucial in our determination of suitable candidates for $\widehat{M}_k(u,\Delta)$.

III.2 Proposition. *Let C, N, u, Δ, ψ and M_k be as in Proposition III.1 and assume in addition that $G(\cdot,u)$ is injective for all $u \in U$. Then*

$$M_k = \bigcap_{\tau=0}^{k} \psi(\tau, X \cap \Delta_{k-\tau}, u|_{[k-\tau;k[}) \tag{8}$$

for all $k \in [0;N]$.

Proof. (8) obviously holds for $k \in \{0,1\}$, so assume (8) holds for some $k \in [1;N[$. Then, using Proposition III.1, we obtain

$$M_{k+1} = \Delta_{k+1} \cap G(M_k,u_k) = \Delta_{k+1} \cap G\left(\bigcap_{\tau=0}^{k} \psi(\tau, X \cap \Delta_{k-\tau}, u|_{[k-\tau;k[}), u_k\right).$$

Injectivity of $G(\cdot,u_k)$ implies $G(A \cap B, u_k) = G(A,u_k) \cap G(B,u_k)$ for any sets A and B. This together with $G(\psi(\tau,\cdot,u|_{[k-\tau;k[}),u_k) = \psi(\tau+1,\cdot,u|_{[k-\tau;k]})$ gives

$$\begin{aligned} M_{k+1} &= \Delta_{k+1} \cap \bigcap_{\tau=0}^{k} \psi(\tau+1, X \cap \Delta_{k-\tau}, u|_{[k-\tau;k+1[}) \\ &= \Delta_{k+1} \cap \bigcap_{\tau=1}^{k+1} \psi(\tau, X \cap \Delta_{k+1-\tau}, u|_{[k+1-\tau;k+1[}). \end{aligned}$$ □

C. Polyhedral over-approximations of attainable sets

We endow the space $\mathbb{R}^n$ with the standard Euclidean product $\langle\cdot|\cdot\rangle$, i.e., $\langle x|y\rangle = \sum_{i=1}^n x_i y_i$ for any $x,y \in \mathbb{R}^n$. The derivative and the inverse of a map f is denoted by f' and f^{-1}, respectively, and f^* is the transpose of f if $f\colon \mathbb{R}^n \to \mathbb{R}^m$ is linear.

III.3 Definition. *For any C^1-diffeomorphism $\Phi\colon V \to W$ between open sets $V,W \subseteq \mathbb{R}^n$, the complementary extension $\Phi^\Diamond\colon V \times \mathbb{R}^n \to W \times \mathbb{R}^n$ of Φ is defined by*

$$\Phi^\Diamond(p,v) = \left(\Phi(p), \left(\Phi'(p)^{-1}\right)^* v\right).$$

We further define

$$P(p,v) = \{x \in \mathbb{R}^n \,|\, \langle v|x-p\rangle \le 0\} \tag{9}$$

for all $p,v \in \mathbb{R}^n$ and set

$$P(\Sigma) = \bigcap_{(p,v)\in\Sigma} P(p,v) \tag{10}$$

for $\Sigma \subseteq \mathbb{R}^n \times \mathbb{R}^n$. In words, (10) is the intersection of the half-spaces (9) represented by pairs $(p,v) \in \Sigma$.

III.4 Definition. *A vector $v \in \mathbb{R}^n$ is normal to $\Omega \subseteq \mathbb{R}^n$ at a boundary point p of Ω if $\langle v|x-p\rangle \le 0$ for all $x \in \Omega$. We call Σ an outer convex approximation of Ω if $\Omega \subseteq P(\Sigma)$, and a supporting convex approximation of Ω, if $p \in \Omega$ and v is normal to Ω at p, for all $(p,v) \in \Sigma$. A finite outer (supporting, resp.) convex approximation is polyhedral.*

Let us now return to the problem of suitable candidates $\widehat{M_k}(u,\Delta)$ for the test (7). If hypothesis (H$_2$) holds and $\Delta_0,\dots,\Delta_N \in C'$, we could define $\widehat{M_k}(u,\Delta)$ to be

$$\widehat{\Delta}_k \cap \bigcap_{\tau=1}^{k} \psi(\tau, \widehat{\Delta}_{k-\tau}, u|_{[k-\tau;k[}), \tag{11}$$

and since $\widehat{\Delta}_N$ and all the sets $\psi(\tau, \widehat{\Delta}_{N-\tau}, u|_{[N-\tau,N[})$ are convex by (H$_2$), the test (7) would be a convex program. The strategy we actually pursue is to take some suitable outer polyhedral approximation of (11) for $\widehat{M_k}(u,\Delta)$. Then the convex program (7) becomes linear, and the sets $\widehat{M_k}(u,\Delta)$ enjoy a recursive description.

III.5 Proposition. *Assume (H$_2$) for some $N \in \mathbb{Z}_+$, as well as (H$_1$), and let $\Delta\colon [0;N] \to C'$, $u\colon [0;N[\to U$ and $\Sigma, S\colon [0;N] \to \mathcal{P}(\mathbb{R}^n \times \mathbb{R}^n)$, where $\mathcal{P}(\cdot)$ denotes the power set. Assume further that Σ_k is a supporting convex approximation of $\widehat{\Delta}_k$ for all $k \in [0;N]$, and*

$$S_0 = \Sigma_0, \tag{12}$$

$$S_k = \Sigma_k \cup G(\cdot, u_{k-1})^{\Diamond}(S_{k-1}) \quad \textit{for } k \in [1;N]. \tag{13}$$

Then, for all $k \in [1;N]$, $G(\cdot,u_{k-1})^{\Diamond}(S_{k-1})$ is an outer convex approximation of $\bigcap_{\tau=1}^{k} \psi(\tau, \widehat{\Delta}_{k-\tau}, u|_{[k-\tau;k[})$, and in particular, S_k is one of (11).

The above result will enable us to iteratively and efficiently compute the sets $\widehat{M_k}(u,\Delta)$ defined earlier. For given u and Δ, such sets correspond to $P(S_k)$, i.e., to the intersection of the half-spaces represented by pairs $(p,v) \in S_k$ of points p and normals v. In view of this implicit representation of polyhedra, (13) says that $\widehat{M_k}(u,\Delta)$ is the intersection, and not the union, of polyhedra $P(\Sigma_k)$ and $P(G(\cdot,u_{k-1})^{\Diamond}(S_{k-1}))$. Moreover, in contrast to $M_k(u,\Delta)$, the set $\widehat{M_k}(u,\Delta)$ is not the intersection of attainable sets of quantizer cells under the dynamics of (1), which is why Propositions III.1 and III.2 cannot be applied to obtain the recursive description in Proposition III.5.

To prove Proposition III.5 we need the following auxiliary result.

III.6 Lemma. *Assume $\Phi\colon V \to W$ is a C^1-diffeomorphism between open sets $V, W \subseteq \mathbb{R}^n$ such that both $\Omega \subseteq V$ and $\Phi(\Omega)$ are convex, and let $p \in \Omega$.*
Then $v \in \mathbb{R}^n$ is normal to Ω at p iff $\left(\Phi'(p)^{-1}\right)^* v$ is normal to $\Phi(\Omega)$ at $\Phi(p)$. In particular, $\Sigma \subseteq \mathbb{R}^n \times \mathbb{R}^n$ is a supporting convex approximation of Ω iff $\Phi^{\Diamond}(\Sigma)$ is one of $\Phi(\Omega)$.

Proof. Let v be normal to Ω at p and define $w = \left(\Phi'(p)^{-1}\right)^* v$ and $q = \Phi(p)$ as well as $\gamma\colon [0,1] \to \mathbb{R}^n\colon t \mapsto \Phi^{-1}(q + t(y-q))$ for some $y \in \Phi(\Omega)$. The map γ is well-defined, differentiable and takes its values in Ω since $q, y \in \Phi(\Omega)$ and $\Phi(\Omega)$ is convex. This implies the map α defined by $\alpha(t) = \langle v|\gamma(t) - p\rangle$ is non-positive as v is normal to Ω at p. Furthermore, α is differentiable with $\alpha(0) = 0$, hence $0 \geq \alpha'(0) = \left\langle v \middle| \left(\Phi^{-1}\right)'(q)(y-q)\right\rangle = \langle w|y-q\rangle$. As y is an arbitrary element of $\Phi(\Omega)$, w is normal to $\Phi(\Omega)$ at q.

For the converse assume w is normal to $\Phi(\Omega)$ at q and observe $\left(((\Phi^{-1})'(q))^{-1}\right)^* w = v$. The first part of this proof applied to Φ^{-1} then shows that v is normal to Ω at p. □

Proof of Proposition III.5. Let $v\colon \mathbb{Z}_+ \to U$ and observe that $\psi(0,p,v) = p$ and $\psi(k+1,p,v) = G(\psi(k,p,v),v_k)$ for all $k \in \mathbb{Z}_+$ and all $p \in X$. Then, by induction, $\psi(k,\cdot,v)$ is a C^1-diffeomorphism between X and an open subset of X, which has two implications. First, by (H$_2$) and Lemma III.6, $\psi(\tau,\cdot,u|_{[k-\tau;k[})^{\Diamond}(\Sigma_{k-\tau})$ is a supporting convex

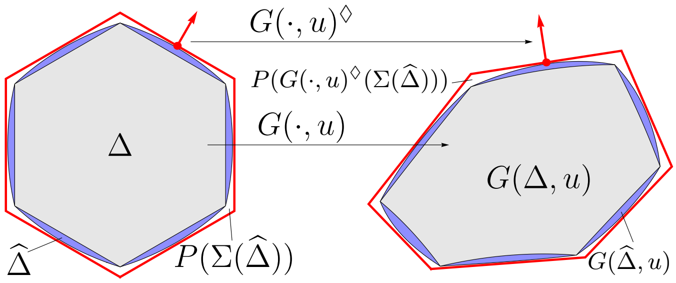


Figure 2. Approximation principle underlying the algorithm in Fig. 3: Let $u \in U$ and consider a cell $\Delta \in C'$ whose image $G(\Delta,u)$ under the nonlinear map $G(\cdot,u)$ is non-convex. Δ is conservatively approximated by some set $\widehat{\Delta}$, and $\widehat{\Delta}$ in turn, by a supporting convex polyhedron $P(\Sigma(\widehat{\Delta}))$. $\Sigma(\widehat{\Delta})$ is mapped under the complementary extension $G(\cdot,u)^\Diamond$. The result, in contrast to images under $G(\cdot,u)$, again represents a convex polyhedron, $P(G(\cdot,u)^\Diamond(\Sigma(\widehat{\Delta})))$. By hypothesis (H$_2$), $G(\widehat{\Delta},u)$ is convex, which guarantees $G(\Delta,u) \subseteq G(\widehat{\Delta},u) \subseteq P(G(\cdot,u)^\Diamond(\Sigma(\widehat{\Delta})))$. The latter set is the one that is actually computed.

approximation of $\psi(\tau,\widehat{\Delta}_{k-\tau},u|_{[k-\tau;k[})$ for all $k \in [0;N]$ and all $\tau \in [0;k]$. Second, we have

$$\psi(k+1,\cdot,v)^\Diamond = G(\cdot,v_k)^\Diamond \circ \psi(k,\cdot,v)^\Diamond \tag{14}$$

for all $k \in \mathbb{Z}_+$, where $\circ$ denotes composition [51], since obviously $(\Phi \circ \Psi)^\Diamond = \Phi^\Diamond \circ \Psi^\Diamond$ for any diffeomorphisms Φ and Ψ whose composition $\Phi \circ \Psi$ is well-defined. We now show

$$G(\cdot,u_{k-1})^\Diamond(S_{k-1}) = \bigcup_{\tau=1}^{k} \psi(\tau,\cdot,u|_{[k-\tau;k[})^\Diamond(\Sigma_{k-\tau}) \tag{15}$$

for all $k \in [1;N]$, which proves the proposition. Observe first that (12) implies (15) for $k=1$, and then assume (15) holds for some $k \in [1;N[$. Then $G(\cdot,u_k)^\Diamond(S_k)$ equals

$$G(\cdot,u_k)^\Diamond(\Sigma_k) \cup \bigcup_{\tau=1}^{k} G(\cdot,u_k)^\Diamond(\psi(\tau,\cdot,u|_{[k-\tau;k[})^\Diamond(\Sigma_{k-\tau}))$$

by (13). The first set in this union is $\psi(1,\cdot,u|_{[k;k+1[})^\Diamond(\Sigma_k)$, and by (14), the union of the last k sets equals $\bigcup_{\tau=1}^{k} \psi(\tau+1,\cdot,u|_{[k-\tau;k+1[})^\Diamond(\Sigma_{k-\tau})$. This implies (15) with k replaced by $k+1$. □

D. Algorithmic solution

We now present an algorithm for efficiently computing discrete abstractions for the quantized system (1),(3), which is based on the geometric idea behind Prop. III.5. See also Fig. 2. Since we are now investigating behaviors, which are sets of signals (u,Δ), the analogs of the sets S_k introduced in Proposition III.5 will depend on u and Δ, which is why we denote them by $S(u|_{[\tau;\tau+k[},\Delta|_{[\tau;\tau+k]})$ in what follows.

III.7 Theorem. *Let be $n \in \mathbb{N}$ and $N \in \mathbb{Z}_+$, assume (H$_1$) and (H$_2$) hold, let $\Sigma(\widehat{\Delta})$ be a supporting polyhedral approximation of $\widehat{\Delta}$, for all $\Delta \in C'$, and let the map $S\colon \bigcup_{k=0}^{N} U^{[0;k[} \times C^{[0;k]} \to \mathcal{P}(\mathbb{R}^n \times \mathbb{R}^n)$ be defined by the output of the algorithm in Fig. 3. Then, for all $k \in [0;N]$, the set*

$$\left\{(u,\Delta) \in (U \times C)^{\mathbb{Z}_+} \,\middle|\, \forall_{\tau\in\mathbb{Z}_+} P(S(u|_{[\tau;\tau+k[},\Delta|_{[\tau;\tau+k]})) \neq \emptyset \right\},$$

which is denoted B_k, is a k-complete discrete abstraction of the behavior of the quantized system (1),(3).

```
Input: $n$, $N$, $U$, $G$, $C$, $C'$; $\Sigma(\widehat{\Delta})$ for each $\Delta \in C'$.
 1: for all $\Delta \in C$ do
 2:   $S(\Delta) := \begin{cases} \Sigma(\widehat{\Delta}), & \text{if } \Delta \in C', \\ \emptyset, & \text{otherwise} \end{cases}$
 3: end for
 4: for $k = 0, \dots, N-1$ do
 5:   for all $u\colon [0;k+1[ \to U$, $\Delta\colon [0;k+1] \to C$ do
 6:     if $S(u|_{[0;k[}, \Delta|_{[0;k]}) = \emptyset$ then
 7:       $S(u,\Delta) := \emptyset$
 8:     else if $\Delta_{k+1} \cap P(G(\cdot,u_k)^{\Diamond}(S(u|_{[0;k[}, \Delta|_{[0;k]}))) = \emptyset$ then
 9:       $S(u,\Delta) := \mathbb{R}^n \times \mathbb{R}^n$
10:     else if $\Delta_{k+1} \notin C'$ then
11:       $S(u,\Delta) := \emptyset$
12:     else
13:       $S(u,\Delta) := \Sigma(\widehat{\Delta}_{k+1}) \cup G(\cdot,u_k)^{\Diamond}(S(u|_{[0;k[}, \Delta|_{[0;k]}))$
14:     end if
15:   end for
16: end for
Output: $S$
```

Figure 3. Algorithm for the computation of outer polyhedral approximations of attainable sets that define a discrete abstraction of quantized system (1),(3).

Proof. First observe the operations to be performed by the algorithm in Fig. 3 are well-defined. In particular, $G(\cdot,u_k)^{\Diamond}$ on lines 8 and 13 of the algorithm shown in Fig. 3 is well-defined by hypotheses (H$_1$) and (H$_2$), and $\Sigma(\widehat{\Delta}_{k+1})$ on line 13 is as well, by the test on line 10.

Denote the behavior of quantized system (1),(3) by B. In order to show B_k is k-complete, let $u\colon \mathbb{Z}_+ \to U$ and $\Delta\colon \mathbb{Z}_+ \to C$, and assume that for all $\tau \in \mathbb{Z}_+$ there is some $(v,\Gamma) \in B_k$ such that $(\sigma^\tau u)|_{[0;k]} = v|_{[0;k]}$ and $(\sigma^\tau \Delta)|_{[0;k]} = \Gamma|_{[0;k]}$. This implies

$$\emptyset \neq P(S(v|_{[0;k[}, \Gamma|_{[0;k]})) = P(S(u|_{[\tau;\tau+k[}, \Delta|_{[\tau;\tau+k]})),$$

thus $(u,\Delta) \in B_k$.

Given arbitrary $K \in [0;N[$, $u\colon [0;K+1[\to U$ and $\Delta\colon [0;K+1] \to C$, we now show

$$P(S(u|_{[0;k[}, \Delta|_{[0;k]})) = \emptyset \text{ implies } M_k = \emptyset \tag{16}$$

for all $k \in [0;K+1]$, where M_k is defined by (8). According to Propositions III.1 and III.2, this implies $B \subseteq B_k$, and hence, proves the theorem.

From the initialization of S on lines 1-3 of the algorithm and hypothesis (H$_2$) it follows that $P(S(\Delta_0)) \neq \emptyset$, thus (16) holds for $k = 0$. Assume now that (16) holds for all $k \in [0;K]$, for some $K \in [0;N[$, as well as $P(S(u,\Delta)) = \emptyset$. In view of lines 6 and 7, this implies $S(u|_{[0;k[}, \Delta|_{[0;k]}) \neq \emptyset$ for all $k \in [0;K+1]$. We further obtain

$$\Delta_{k+1} \cap P(G(\cdot,u_k)^{\Diamond}(S(u|_{[0;k[}, \Delta|_{[0;k]}))) = \emptyset \tag{17}$$

for $k = K$. Otherwise, $S(u,\Delta)$ would have been assigned its value on line 13, i.e.,

$$S(u|_{[0;k+1[}, \Delta|_{[0;k+1]}) = \Sigma(\widehat{\Delta}_{k+1}) \cup G(\cdot,u_k)^{\Diamond}(S(u|_{[0;k[}, \Delta|_{[0;k]})) \tag{18}$$

for $k = K$; thus the left hand side of (17) would be a subset of $P(S(u, \Delta)) = \emptyset$, which is a contradiction.

Now assume (17) also holds for some $k \in [0; K[$. Then $S(u|_{[0;k+1[}, \Delta|_{[0;k+1]})$ is assigned its value on line 9, hence $P(S(u|_{[0;k+1[}, \Delta|_{[0;k+1]})) = \emptyset$. From this and (16) we obtain $M_{k+1} = \emptyset$, and Proposition III.1 yields $M_{K+1} = \emptyset$. Thus, (16) holds for $k = K + 1$.

If, on the other hand, (17) does not hold for any $k \in [0; K[$, then, in view of lines 2, 6, 7, 10 and 11, we obtain $\Delta_\tau \in C'$ for all $\tau \in [0; K]$, $S(\Delta_0) = \Sigma(\widehat{\Delta}_0)$, as well as (18) for all $k \in [0; K[$. Proposition III.5 then shows that the left hand side of (17) for $k = K$ contains M_{K+1} as a subset, so (16) holds for $k = K + 1$, and we are done. □

III.8 Corollary. *Under the hypotheses of Theorem III.7 and for all $k \in [0; N]$, the requirement*

$$\exists_{\Delta\colon \mathbb{Z}_+ \to C} \big((u, \Delta) \in B_k \text{ and } \forall_{k \in \mathbb{Z}_+} x_k \in \Delta_k \big)$$

for sequences $(u, x)\colon \mathbb{Z}_+ \to U \times \mathbb{R}^n$ defines an abstraction of the behavior of the discrete-time system (1).

We remark that the algorithm in Fig. 3 contains just two nontrivial operations which need to be performed repeatedly, namely, the determination of the set

$$G(\cdot, u_k)^{\Diamond}(S(u|_{[0;k[}, \Delta|_{[0;k]})), \tag{19}$$

which appears on lines 8 and 13, and the test for emptiness on line 8. The latter can be efficiently performed using linear programming techniques, since both Δ_{k+1} and $P(G(\cdot, u_k)^{\Diamond}(S(u|_{[0;k[}, \Delta|_{[0;k]})))$ are convex polyhedra. According to Definition III.3, the former operation requires an evaluation of the function $G(\cdot, u_k)$ and the solution of a linear system of equations for each element $(p, v) \in S(u|_{[0;k[}, \Delta|_{[0;k]})$,

$$\tilde{p} = G(p, u_k), \tag{20a}$$

$$v = D_1 G(p, u_k)^* \tilde{v}, \tag{20b}$$

in order to obtain an element $(\tilde{p}, \tilde{v})$ of (19), which represents one half-space in the outer convex approximation (19). Here, $D_i f$ denotes the partial derivative of f with respect to the ith argument.

In order to estimate the computational complexity of the algorithm in Fig. 3, we assume for simplicity that each of the sets $\widehat{\Delta}$ is approximated by m supporting half-spaces, i.e., $m = |\Sigma(\widehat{\Delta})|$ for all $\Delta \in C'$, where $|\cdot|$ denotes cardinality. It is then easy to see that for any given $k \in [0; N[$, the number of half-spaces needed to define all the sets (19) is at most $m|C||U|^{k+1}$, and these sets are represented by at most $(k + 1)m$ half-spaces each. To estimate the number of tests for emptiness, we additionally assume that there is a constant $\lambda > 0$, independent of $|C|$, such that the following holds. For any given set of the form (19), the test on line 8 has to be performed for at most λ cells $\Delta_{k+1} \in C$, and the set of these candidate cells can be provided in constant time. This holds, in particular, if the cells in C' are congruent compacta arranged in a regular grid. Then, for any given k, the number of tests on line 8 is bounded by $\lambda^{k+1}|C||U|^{k+1}$. Note here that the values $\emptyset$ and $\mathbb{R}^n \times \mathbb{R}^n$, which may be assigned on lines 9 and 11, play a role similar to zeros in sparse matrices, and thus, these values do not need to be stored and computations on them do not need to actually be performed [52].

In summary, the algorithm in Fig. 3 requires the solution of $O(m|C||U|^N)$ instances of (20) and of $O(\lambda^N|C||U|^N)$ linear feasibility problems in n variables with at most $(N+1)m$ inequalities each, where $O(\cdot)$ is the usual asymptotic notation [53]. The parameters m

and $|C|$ depend on the dimension n of the state space of (1), with $|C|$ typically growing exponentially. Therefore, the computational effort has to be expected to grow rapidly with n, a problem that is common to all grid based methods for the computation of abstractions, e.g. [1], [8], [26], [27], [32].

We remark that apart from an increasing computational effort, application of the algorithm shown in Fig. 3 in dimensions exceeding 2 does not pose any particular difficulties. This is obvious for the operations on lines 8 and 13, which we have already discussed, and also holds for the remaining operations. Specifically, for the computation of the supporting polyhedral approximations $\Sigma(\widehat{\Delta})$ on line 2, several methods are available for a large class of sets $\widehat{\Delta}$ [53].

Finally, we would like to emphasize again that convexity of certain attainable sets is an important requirement for the correctness of the algorithm in Fig. 3, see hypothesis (H_2). While for linear systems that requirement is always met by the choice $\widehat{\Delta} = \Delta$, the results of section IV will show how to meet it in the presence of non-linearities.

E. Sampled systems

Here we consider the case that (1) arises from a continuous-time system (2) under sampling. More formally, let a continuous-time control system (2) with $F\colon X \times V \to \mathbb{R}^n$ and a set U of input signals be given, where $X \subseteq \mathbb{R}^n$, $V \subseteq \mathbb{R}^m$, each $u \in U$ is a piecewise continuous map $u\colon [0, T] \to V$, and $T > 0$ is the *sampling period*. A map $v\colon \mathbb{R}_+ \to V$ is an *admissible input signal* for (2), generated by $u\colon \mathbb{Z}_+ \to U$, if $v(t) = u_k(t - kT)$ for all $k \in \mathbb{Z}_+$ and all $t \in [kT, (k + 1)T[$. The set of admissible input signals for (2) is denoted $\mathcal{V}$ in the sequel. We assume the following.

($\mathbf{H_3}$) $X \subseteq \mathbb{R}^n$ is open, the right hand side F of (2) is continuously differentiable with respect to its first argument and continuous. Furthermore, for any $x_0 \in X$ and any admissible input signal $v \in \mathcal{V}$, the solution of the initial value problem composed of (2) and the initial condition $x(0) = x_0$ is extendable to the entire time axis $\mathbb{R}_+$.

Discrete-time system (1) is called the *sampled system* associated with (2) if its right hand side is given by

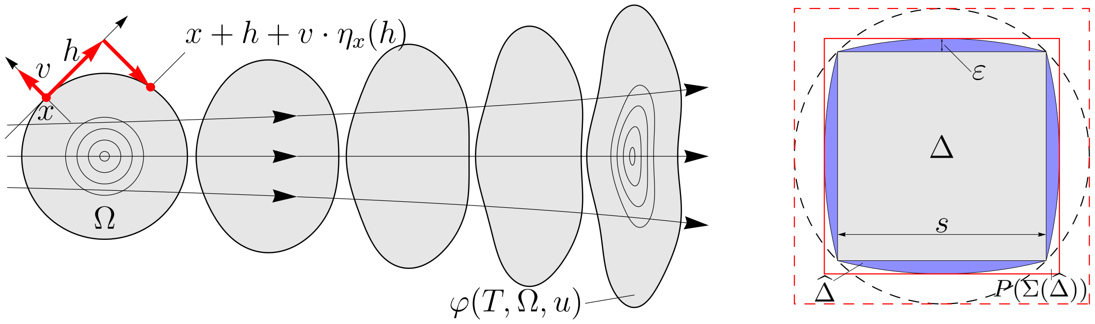
$$G(x, u) = \varphi(T, x, u)$$

for all $x \in X$ and all $u \in U$, where φ is the *general solution* of (2), i.e., $\varphi(t, x_0, v)$ is the value at time t of the solution of the initial value problem composed of (2) and the initial condition $x(0) = x_0$.

Obviously, the sampled system (1) associated with (2) fulfills (H_1) if (2) fulfills (H_3), and $\psi(k, x, u) = \varphi(kT, x, v)$ for all $x \in X$ and all $k \in \mathbb{Z}_+$, whenever v is an admissible input signal for (2) generated by the sequence $u\colon \mathbb{Z}_+ \to U$ and ψ is the general solution of (1). Hence, our results for (1), including the algorithm in Fig. 3, can be directly applied to the sampled system (1) associated with (2) if the latter satisfies hypothesis (H_3). In particular, (20) can be efficiently solved even though the right hand side G of the sampled system (1) is not explicitly given. The solution is obtained through solving an initial value problem in a $2n$-dimensional ordinary differential equation (ODE) over a single sampling interval:

III.9 Proposition. *Let (1) be the sampled system associated with (2) for sampling period $T > 0$, and assume (H_3). Then*

$$G(\cdot, u)^{\Diamond}(p, v) = (x(T), y(T))$$



(a) (b)

Figure 4. (a) Geometric idea behind our derivations in Section IV for the continuous-time system (2): If Ω is an Euclidean ball of radius r and the right hand side F of (2) is of class $C^{1,1}$, then the attainable set $\varphi(T, \Omega, u)$ is convex whenever T or r is small enough. This idea does not extend to smooth, strictly convex sets Ω, nor to right hand sides F of class C^1. (b) The smallest intersection $\widehat{\Delta}$ of a finite number of closed balls of radius r containing a polyhedron Δ is a subset of any r-convex ellipsoid (dashed) containing Δ.

for all $u \in U$, $p \in X$ and $v \in \mathbb{R}^n$, where (x, y) denotes the solution of the initial value problem

$$\dot{x}(t) = F(x(t), u(t)), \tag{21a}$$

$$\dot{y}(t) = -D_1 F(x(t), u(t))^* y(t), \tag{21b}$$

$$x(0) = p, \quad y(0) = v. \tag{21c}$$

Proof. Assume u is continuous and let φ denote the general solution of (2). (H$_3$) implies φ is continuously differentiable, $X := D_2\varphi(\cdot, p, u)$ fulfills the variational equation $\dot{X}(t) = D_1 F(x(t), u(t)) X(t)$, and $X(0) = \mathrm{id}$, e.g. [54]. In particular, $G(\cdot, u)$ is a C^1-diffeomorphism, so its complementary extension $G(\cdot, u)^\Diamond$ is well-defined. Furthermore, $(X(\cdot)^{-1})^*$ fulfills the adjoint equation (21b), e.g. [54]. Thus, $(D_1 G(p, u)^{-1})^* v = (X(T)^{-1})^* v = y(T)$. The extension to piecewise continuous u is obvious. □

IV. Convexity of attainable sets

In this section we will investigate the convexity of attainable sets of control systems (1) and (2). To begin with, we briefly explain the geometric idea behind our derivations using the example of the continuous-time system (2). Consider a set $\Omega \subseteq \mathbb{R}^n$ of class C^2, denote its boundary by $\partial\Omega$, let $x \in \partial\Omega$ be an arbitrary boundary point, and let v be a unit-length normal to Ω at x. Let η_x be a C^2-map defined on the tangent space of $\partial\Omega$ at x that represents the boundary $\partial\Omega$ locally about the point x in local coordinates, with the origin located at x. That is, η_x is such that in a neighborhood of x we have $y \in \partial\Omega$ iff there is a tangent vector h to $\partial\Omega$ at x such that $y = x + h + v \cdot \eta_x(h)$. See Fig. 4(a). The map η_x is locally uniquely determined by Ω and satisfies $\eta_x(0) = 0$ and $\eta_x'(0) = 0$. Moreover, Ω is convex iff $\eta_x''(0)$ is negative semi-definite for every $x \in \partial\Omega$ [47], where η_x'' denotes the second order derivative of η_x. Consequently, if the right hand side F of (2) is of class C^2, the issue of convexity of attainable sets can be decided by studying the evolution of $\eta_x''(0)$ under the dynamics of (2). The realization of that idea in the case that Ω is a Euclidean ball centered at some point x_0 reveals that the attainable set $\varphi(T, \Omega, u)$ is convex whenever the time T or the radius r of Ω is small enough [47]. See Fig. 4(a). Moreover, bounds on T and r can be derived from properties of the right hand side F of

(2). These results generalize to ellipsoids at the place of balls and can also be generalized to the case of $C^{1,1}$-smoothness by using suitably generalized second order derivatives [47]. They do not, however, extend to smooth, strictly convex sets, nor to right hand sides of class C^1. In particular, attainable sets $\varphi(T, \Omega, u)$ can then be non-convex for any time $T > 0$.

In the present section, we will replace ellipsoids by strongly convex sets. Here, the set $\Omega \subseteq \mathbb{R}^n$ is *strongly convex of radius* r, or r*-convex* for short, if it is an intersection of a family of closed balls of radius $r > 0$, i.e., if

$$\Omega = \bigcap_{x \in M} \bar{B}(x, r) \tag{22}$$

for some $M \subseteq \mathbb{R}^n$, where $\bar{B}(x, r)$ denotes the closed Euclidean ball of radius r centered at x. Ω is *strongly convex* if it is r-convex for some $r > 0$ [55], [56].

In view of the method proposed in Section III, the use of strongly convex rather than ellipsoidal supersets of quantizer cells allows for more precise approximations of attainable sets, and thus, for more accurate abstractions. Indeed, in contrast to the case of ellipsoidal supersets, the error ε by which $P(\Sigma(\widehat{\Delta}))$ approximates the cell Δ in Fig. 4(b) is quadratic in the edge length s of Δ, and it can be shown that this property carries over to approximations of attainable sets of Δ. See also Fig. 2.

We will also extend previous results to the discrete-time case (1). Our results not only allow verification of the requirements for the correctness of the algorithm of section III when a particular quantizer is given, but they also help in constructing admissible quantizers. In particular, we show that if hypothesis (H_1) is fulfilled with sufficient smoothness and $Y \subseteq \mathbb{R}^n$ is a compact, full-dimensional, convex polyhedron, then choosing sufficiently small scaled and translated copies of Y as operating range quantizer cells will guarantee that the stated requirements of section III are met.

As the problems investigated in this section become trivial in dimension 1, we assume a multidimensional setting, i.e., $n \geq 2$ throughout this section.

A. Convexity of diffeomorphic images of strongly convex sets

We first present a sufficient condition for the diffeomorphic image of a strongly convex set to be itself convex, which will be the basis of all subsequent results. In what follows, we write $x \perp y$ if $\langle x|y \rangle = 0$ and denote by $\|\cdot\|$ the Euclidean norm of both vectors and linear maps. The closure, interior and boundary of a set $M \subseteq \mathbb{R}^n$ is denoted $\operatorname{cl} M$, $\operatorname{int} M$ and ∂M, respectively. We set $fh^k := f(h, \ldots, h)$ if f is k-linear.

IV.1 Proposition. *Let $\Phi \colon U \to V$ be a $C^{1,1}$-diffeomorphism between open sets $U, V \subseteq \mathbb{R}^n$ and $\Omega \subseteq U$ be r-convex, $\Omega \neq \mathbb{R}^n$. Assume that for each $x \in \partial\Omega$ there is a unit length normal v to Ω at x such that*

$$\limsup_{t \to 0, t > 0} \frac{\langle v | \Phi'(x)^{-1}(\Phi'(x + t\xi) - \Phi'(x))\xi \rangle}{t} < \frac{1}{r}\|\xi\|^2 \tag{23}$$

holds for all $\xi \perp v$, $\xi \neq 0$. Then $\Phi(\Omega)$ is convex.

It should be noted that the left hand side of (23) equals $\langle v | \Phi'(x)^{-1}\Phi''(x)\xi^2 \rangle$ if Φ is of class C^2. In addition, if (23) were not a strict inequality and if Ω is a closed ball of radius r, the condition is known to be necessary and sufficient for the convexity of $\Phi(\Omega)$ [47]. However, this does not prove the proposition, despite representation (22). Indeed, (23) is only required to hold at boundary points x of Ω. Hence, even if all balls that appear in

(22) are in the domain of definition U of Φ, (23) may very well be violated at boundary points of these balls.

In the course of proving Proposition IV.1 we will say that Ω is *weakly supported at* $p \in \partial\Omega$ *locally* whenever there is some neighborhood U of p and a non-zero normal to $\Omega \cap U$ at p [49]. Further, we will call $f\colon U \to \mathbb{R}$ a $C^{1,1}$*-submersion on its zero set* if the following holds: f is continuous on the open set $U \subseteq \mathbb{R}^n$, and for every zero x of f, f is of class $C^{1,1}$ on a neighborhood of x and $f'(x)$ is surjective.

IV.2 Lemma. *Let* $g\colon U \subseteq \mathbb{R}^n \to \mathbb{R}$ *be a* $C^{1,1}$*-submersion on its zero set,* $\Omega = \{x \in U \mid g(x) \leq 0\}$, *and assume* $g(0) = 0$ *and*

$$\liminf_{t \to 0, t>0} \frac{g'(th)h}{t} > 0 \tag{24}$$

for all $h \in \ker g'(0) \setminus \{0\}$*. Then* Ω *is weakly supported at* 0 *locally.*

Proof. Set $v = g'(0)^*/\|g'(0)\|$. An application of the implicit function theorem to the equation $g(h + \lambda v) = 0$ for $h \in \ker g'(0)$ and $\lambda \in \mathbb{R}$ shows that Ω can be represented locally about 0 by a map $\eta\colon W \subseteq \ker g'(0) \to \mathbb{R}$ of class $C^{1,1}$, W an open neighborhood of the origin. That is, for h and λ small enough we have $h + \lambda v \in \Omega$ iff $\lambda \leq \eta(h)$. Combine this with the identity $\langle v|h + \lambda v\rangle = \lambda$ and the definition of weak local support to see that it suffices to show $\eta(h) \leq 0$ for all sufficiently small h. In order to prove the latter, first observe that $\eta(0) = 0$ and $\eta'(0) = 0$. Then differentiate the identity $g(h + \eta(h)v) = 0$ with respect to h and use the Lipschitz continuity of g' to obtain

$$\limsup_{t \to 0, t>0} \eta'(th)h/t = -\|g'(0)\|^{-1} \liminf_{t \to 0, t>0} g'(th)h/t$$

for all $h \in \ker g'(0)$. If g is of class C^2, then so is η, the left hand side of the latter equation equals $\eta''(0)h^2$, and the claim follows from (24). If g is merely $C^{1,1}$, use again (24) and apply [57, Theorem 3.2]. □

Proof of Proposition IV.1. The claim is trivial for $\Omega = \emptyset$ and Ω a singleton, so we assume Ω contains at least two points. Then Ω has nonempty interior by Lemma A.1 in the Appendix. In addition, Ω is compact and convex. Hence $\Omega = \operatorname{cl}(\operatorname{int}(\Omega))$ and $\operatorname{int}(\Omega)$ is connected, and these properties are preserved under diffeomorphisms. Moreover, $\operatorname{int}(\Phi(\Omega)) = \Phi(\operatorname{int}(\Omega))$ since Φ is a diffeomorphism.

We will show below that $\operatorname{int}(\Phi(\Omega))$ is weakly supported at each of its boundary points locally. Then, since that set is also open and connected, it is convex [49, Theorem 4.10], which implies its closure $\Phi(\Omega)$ is also convex.

Let $x \in \partial\Omega$ be arbitrary and v be as in the statement of the proposition, and assume $x = \Phi(x) = 0$ without loss of generality. Then $\Omega \subseteq \bar{B}(-rv, r)$ since Ω is r-convex and compact [55, Proposition 3.1]. Now define $f(z) = \|z + rv\|^2 - r^2$ and $g = f \circ \Phi^{-1}$ to observe that $g(y) \leq 0$ is equivalent to $y \in \Phi(\bar{B}(-rv, r))$, hence

$$\Phi(\Omega) \subseteq \{y \in V \mid g(y) \leq 0\}\,. \tag{25}$$

We claim that the set on the right hand side of (25) is weakly supported at the origin locally. To prove this, first observe that g is a $C^{1,1}$-submersion on its zero set since f is one and Φ is a $C^{1,1}$-diffeomorphism, and that $g(0) = 0$. Then differentiate the identity $f = g \circ \Phi$, observe $f'(t\xi)\xi/t = 2\|\xi\|^2$, and use the Lipschitz continuity of g' and the continuity of Φ' to see that $2\|\xi\|^2$ equals

$$\liminf_{t \to 0, t>0} \left(g'(th)h/t + 2r \left\langle v \middle| \Phi'(0)^{-1}(\Phi'(t\xi) - \Phi'(0))\xi \right\rangle /t\right)$$

whenever $h = \Phi'(0)\xi$. The identity $g'(0)\Phi'(0)\xi = 2r \langle v|\xi \rangle$ and (23) for all $\xi \perp v$, $\xi \neq 0$ imply (24) for all $h \in \ker g'(0) \setminus \{0\}$, and an application of Lemma IV.2 proves our claim.

Now, since the origin is also a boundary point of $\Phi(\Omega)$, and since the right hand side of (25) is weakly supported at the origin locally, so is $\Phi(\Omega)$, and hence, $\operatorname{int}(\Phi(\Omega))$. □

B. Convexity of attainable sets of discrete-time systems

We next present a result that enables us to verify hypothesis (H_2), and hence, to establish the correctness of the algorithm proposed in section III for the computation of discrete abstractions of the quantized system (1),(3), whenever a particular quantizer together with its system C' of operating range cells is given. In what follows, $D_i^j f$ denotes the partial derivative of order j with respect to the ith argument, of the map f.

IV.3 Theorem. *Assume (H_1) with smoothness $C^{1,1}$, let ψ denote the general solution of (1), and let $N \in \mathbb{N}$ and $\Omega \subseteq X$ be r-convex with $\Omega \neq \mathbb{R}^n$. Assume that there are $L_1, L_2 \in \mathbb{R}$ such that*

$$L_1 \geq \alpha_+(D_1G(x,w))^2/\alpha_-(D_1G(x,w)), \tag{26}$$

$$L_2 \geq \limsup_{h\to 0} \frac{\|D_1G(x,w)^{-1}D_1G(x+h,w) - \operatorname{id}\|}{\|h\|} \tag{27}$$

for all $(x,w) \in \psi([0;N[\,,\Omega,U^{\mathbb{Z}_+}) \times U \subseteq X \times U$, where $\alpha_+(A)$ and $\alpha_-(A)$ denote the maximum and minimum, respectively, singular values of A. Then the attainable set $\psi(k,\Omega,u)$ is convex for all $k \in [0;N]$ and all $u\colon \mathbb{Z}_+ \to U$ if

$$rL_2 \sum_{\tau=0}^{N-1} L_1^\tau \leq 1. \tag{28}$$

Proof. We may assume Ω contains at least two points as well as $k = N$ without loss of generality. By our hypotheses on the right hand side G of (1), the map $\Phi := \psi(N,\cdot,u)$ is a $C^{1,1}$-diffeomorphism between an open neighborhood of Ω and an open subset of X. We first prove the claim under the assumption that (28) is strict by applying Prop. IV.1 to Φ:

Let $x \in \partial\Omega$, v any unit length normal to Ω at x, and $\xi \perp v$. For t small enough and $k \in [0;N]$ define $y_k(t) = D_2\psi(k, x+t\xi, u)\xi$. Then $y_0(t) = \xi$, and the sequence $y(t)$ solves the variational equation to (1) along $\psi(\cdot, x+t\xi, u)$, i.e.,

$$y_{k+1}(t) = D_1G(\psi(k, x+t\xi, u), u_k)y_k(t) \tag{29}$$

for all $k \in [0;N[$. Next define $z_k(t) = (y_k(t) - y_k(0))/t$ for $t > 0$ small enough. Then $z_0(t) = 0$, and the sequence $z(t)$ solves another linear difference equation, namely,

$$z_{k+1}(t) = D_1G(\psi(k,x,u), u_k)z_k(t) + b_k \tag{30}$$

for all $k \in [0;N[$, where b_k denotes

$$(D_1G(\psi(k, x+t\xi, u), u_k) - D_1G(\psi(k,x,u), u_k))\, y_k(t)/t.$$

Note that in the case of C^2-smoothness, if we let t tend to 0, then (30) reduces to the variational equation (whose solution is $D_2^2\psi(k,x,u)\xi^2$) of the variational equation (29). Now observe $(k,k_0) \mapsto D_2\psi(k,x,u)D_2\psi(k_0,x,u)^{-1}$ is the transition matrix of the homogeneous system associated with (30), use the identity

$$\Phi'(x)^{-1}(\Phi'(x+t\xi) - \Phi'(x))\xi/t = D_2\psi(N,x,u)^{-1}z_N(t) \tag{31}$$

and apply the discrete variation of constants formula [58] to (30) to see that the left hand side of (31) equals

$$\sum_{\tau=0}^{N-1} D_2\psi(\tau,x,u)^{-1} D_1 G(\psi(\tau,x,u),u_\tau)^{-1} b_\tau. \tag{32}$$

From the variational equation of (1) along $\psi(\cdot,x,u)$ we obtain

$$\begin{aligned}\|D_2\psi(\tau+1,x,u)\| &\leq \alpha_+(D_1G(p,u_\tau))\|D_2\psi(\tau,x,u)\|,\\ \|D_2\psi(\tau+1,x,u)^{-1}\| &\leq \frac{\|D_2\psi(\tau,x,u)^{-1}\|}{\alpha_-(D_1G(p,u_\tau))},\end{aligned}$$

where $p = \psi(\tau,x,u)$; hence, by our hypothesis (26),

$$\|D_2\psi(\tau,x,u)^{-1}\| \cdot \|D_2\psi(\tau,x,u)\|^2 \leq L_1^\tau \tag{33}$$

for all $x \in \Omega$, $u\colon \mathbb{Z}_+ \to U$ and $\tau \in [0;N[$.

Let $\varepsilon > 0$ be arbitrary. Then $\|D_2\psi(\tau,x+t\xi,u)\| \leq (1+\varepsilon)\|D_2\psi(\tau,x,u)\|$ whenever t is small enough. Use this fact, the bound (27), the mean value theorem, and (33) to obtain the upper bound $(1+\varepsilon)^3 L_2\|\xi\|^2 \sum_{\tau=0}^{N-1} L_1^\tau$ for the norm of (32), for all $x \in \Omega$, $u\colon \mathbb{Z}_+ \to U$ and all $t > 0$ small enough. Now let ε tend to 0 to see that the strict variant of (28) implies (23), hence the convexity of $\Phi(\Omega)$.

To complete the proof, assume Ω is of form (22) and define

$$\Theta(s) = \bigcap_{x\in M} \bar{B}(x,s) \tag{34}$$

for $s > 0$. Then $\Phi(\Theta(s))$ is convex for all $s < r$ by the first part of this proof. By Lemma A.2, $\Theta(s)$ converges to Ω in Hausdorff distance, and that property is preserved under diffeomorphisms. Consequently, $\Phi(\Omega)$ is the limit of convex sets, and thus, is itself convex [59]. □

We remark that the hypotheses of Theorem IV.3 can be verified by inspection of the right hand side G of (1). Indeed, suitable constants L_1 and L_2 are obtained from estimates of singular values of $D_1G(x,w)$ and of a Lipschitz constant of $D_1G(x,w)^{-1}D_1G(y,w)$ with respect to y, respectively. In this regard, note also that L_2 is just a bound on $\|D_1G(x,w)^{-1}D_1^2G(x,w)\|$ if the right hand side G is of class C^2 with respect to its first argument.

C. Construction of admissible quantizers

We now turn to the question of how to construct an admissible quantizer. Let there be given some $N \in \mathbb{N}$ and a compact subset $K \subseteq X$ of the state space X of the discrete-time system (1) together with an open neighborhood $V \subseteq X$ of K. Intuitively, N is the memory span of an abstraction we seek to compute, K is the intended operating range of the quantizer, and V can be thought of as a maximal operating range, i.e., $X \setminus V$ should be covered by overflow symbols. Of course, our choice of N, K and V would depend on particularities of the problem we intend to solve.

In addition, let there be given a full-dimensional, convex polyhedron $Y \subseteq \mathbb{R}^n$ together with a strongly convex set $\hat{Y} \neq \mathbb{R}^n$ containing Y as a subset. Denote the general solution of the discrete-time system (1) by ψ. We will first choose a finite set C' of scaled and translated copies of Y that cover K, i.e.,

$$C' = \{z + \lambda Y \mid z \in Z\}, \tag{35}$$

$$K \subseteq Z + \lambda Y \tag{36}$$

for some $\lambda > 0$ and some finite subset $Z \subseteq \mathbb{R}^n$, and then supplement C' by overflow symbols to obtain a finite cover C of $\mathbb{R}^n$ for which (H$_2$) holds. Our choice will further guarantee $Z + \lambda\widehat{Y} \subseteq V$ and that the attainable sets $\psi(k, z + \lambda\widehat{Y}, u)$ are convex for all $k \in [1; N]$, $z \in Z$, and $u\colon\ [0; k[\to U$.

Assume without loss of generality that the origin is an interior point of Y and $\widehat{Y}$ is 1/2-convex, and denote the distance between K and $\mathbb{R}^n \setminus V$ by d. Then $d > 0$ as K is compact and V is open, and $K + \lambda\widehat{Y}$ is compact and contained in V for any $\lambda \in\ ]0, d]$. Hence $K' := \psi([0; N[\,, K + \lambda\widehat{Y}, U^{\mathbb{Z}_+})$ is compact if U is finite. If (H$_1$) holds with smoothness $C^{1,1}$, then $G(\cdot, w)$ is a $C^{1,1}$-diffeomorphism, so we may choose L_1, L_2 and $\lambda > 0$ such that $\lambda/2 \leq r := (L_2 \sum_{\tau=0}^{N-1} L_1^{\tau})^{-1}$ and (26) and (27) hold for all $(x, w) \in K' \times U$, as well as $K + \lambda\widehat{Y} \subseteq V$. Then $\lambda\widehat{Y}$ is r-convex, thus attainable sets $\psi(k, z + \lambda\widehat{Y}, u)$ are convex for all $k \in [1; N]$, $z \in K$ and $u\colon\ [0; k[\to U$ by Theorem IV.3.

Since $\lambda > 0$, K is compact and the origin is an interior point of Y, we can find a finite subset $Z \subseteq K$ for which (36) holds, and we could even guarantee $K \subseteq Z + \lambda \operatorname{int} Y$ if necessary. Finally, Lemma A.3 in the Appendix shows that if the set C' is defined by (35), it can be supplemented by convex polyhedra to obtain a finite covering of $\mathbb{R}^n$. We have thus proved the following result, which easily extends to the case of a compact rather than finite input alphabet.

IV.4 Theorem. *Let the input alphabet U of the discrete-time system (1) be finite and assume (H$_1$) with smoothness $C^{1,1}$. Let further be given some $N \in \mathbb{N}$, a compact subset $K \subseteq X$, an open neighborhood $V \subseteq X$ of K, as well as a full-dimensional, convex polyhedron $Y \subseteq \mathbb{R}^n$ together with a strongly convex set $\widehat{Y} \subseteq \mathbb{R}^n$ for which $Y \subseteq \widehat{Y} \neq \mathbb{R}^n$. Then there is a finite subset $Z \subseteq \mathbb{R}^n$, some $\lambda > 0$, and a superset C of the set C' defined by (35) such that (H$_2$) and*

$$K \subseteq Z + \lambda Y \subseteq Z + \lambda\widehat{Y} \subseteq V$$

hold. Moreover, $\Delta \cap \operatorname{int} \Delta' = \emptyset$ for all $\Delta \in C \setminus C'$ and all $\Delta' \in C'$, and one may additionally require $\Delta \cap K = \emptyset$ for all overflow symbols $\Delta \in C \setminus C'$.

D. Convexity of attainable sets of sampled systems

We finally provide two results useful for sampled systems.

IV.5 Theorem. *Assume (H$_3$), let the right hand side F of (2) be of class $C^{1,1}$ with respect to its first argument, and let φ denote the general solution of (2). Let $t > 0$ and $\Omega \subseteq X$ be r-convex with $\Omega \neq \mathbb{R}^n$. Further assume that there are $M_1, M_2 \in \mathbb{R}$ such that*

$$M_1 \geq 2\mu_+(D_1F(x, w)) - \mu_-(D_1F(x, w)),$$
$$M_2 \geq \limsup_{h \to 0} \frac{\|D_1F(x + h, w) - D_1F(x, w)\|}{\|h\|}$$

for all $(x, w) \in \varphi([0, t]\,, \Omega, \mathcal{V}) \times V \subseteq X \times V$, where $\mu_+(A)$ and $\mu_-(A)$ denote the maximum and minimum, respectively, eigenvalues of the symmetric part $(A + A^*)/2$ of A. Then the *attainable set $\varphi(\tau, \Omega, v)$ is convex for all $\tau \in [0,t]$ and all admissible input signals $v \in \mathcal{V}$ if*

$$rM_2 \int_0^t \exp(M_1 \rho)\, d\rho \leq 1. \tag{37}$$

Proof. We may assume Ω contains at least two points as well as $\tau = t$ without loss of generality. By our hypotheses on the right hand side F of (2), the map $\Phi := \varphi(t, \cdot, v)$ is a $C^{1,1}$-diffeomorphism between an open neighborhood of Ω and an open subset of X. We assume Ω is of form (22), define $\Theta(s)$ for $s > 0$ by (34), and prove $\varphi(t, \Theta(s), v)$ is convex for any $s \in]0, r[$ by applying Proposition IV.1 to Φ. The theorem then follows from Lemma A.2.

To this end, set $I = [0,t]$ and $X' = \varphi(I, \operatorname{int}\Omega, v)$, and define $f\colon I \times X' \to \mathbb{R}^n$ by $f(\tau, x) = F(x, v(\tau))$. Since X' is an open neighborhood of $\varphi(I, \Theta(s), v)$, the ODE $\dot{x} = f(t,x)$ fulfills the hypothesis of [47, Theorem 3]. The proof of the latter result shows that if v is continuous, then for any $x \in X'$ and any $\varepsilon > 0$ we have $\|\Phi'(x)^{-1}(\Phi'(x+h) - \Phi'(x))\| \leq (1+\varepsilon)^2 M_2 \|h\| \int_0^t \exp(M_1\rho)\, d\rho$ for all sufficiently small h. The extension to piecewise continuous v is straightforward. Then (37) implies (23) with s substituted for r and ζ substituted for v, for any $x \in \partial\Theta(s)$ and any $\zeta, \xi \in \mathbb{R}^n$ with $\|\zeta\| = 1$ and $\xi \neq 0$. Thus $\Phi(\Theta(s))$ is convex by Proposition IV.1. □

IV.6 Theorem. *Assume (H$_3$), let the right hand side F of (2) be of class C^2 with respect to its first argument, and let φ, t, Ω, and r be as in Theorem IV.5. Assume further that there is a constant L_2 such that*

$$\left\| \int_0^\delta D_2\varphi(\tau, x, v)^{-1} D_1^2 F(p(\tau), v(\tau))\, (D_2\varphi(\tau, x, v)h)^2\, d\tau \right\| \leq L_2 \|h\|^2 \tag{38}$$

for all $x \in \Omega$, $\delta \in [0,t]$, $v \in \mathcal{V}$ and $h \in \mathbb{R}^n$, where $p(\tau) = \varphi(\tau, x, v)$. Then the attainable set $\varphi(\tau, \Omega, v)$ is convex for all $\tau \in [0,t]$ and all admissible input signals $v \in \mathcal{V}$ if $rL_2 \leq 1$.

Proof. As in the proof of Theorem IV.5, we assume Ω contains at least two points and $\tau = t$, define $\Theta(s)$ by (34), and observe $\Phi := \varphi(t, \cdot, v)$ is a C^2-diffeomorphism. Let $x \in X$, $h \in \mathbb{R}^n$, $v \in \mathcal{V}$, and define $y(t) = D_2\varphi(t, x, v)h$. Then $y(0) = h$, and y solves the variational equation to (2) along $\varphi(\cdot, x, v)$, i.e.,

$$\dot{y}(t) = D_1F(\varphi(t,x,v), v(t))y(t) \tag{39}$$

for all $t \geq 0$. Next define $z(t) = D_2^2\varphi(t,x,v)h^2$. Then $z(0) = 0$, and z solves another linear ODE, namely,

$$\dot{z}(t) = D_1F(\varphi(t,x,v), v(t))z(t) + D_1^2F(\varphi(t,x,v), v(t))y(t)^2 \tag{40}$$

for all $t \geq 0$. (Note that x is a parameter rather than an initial value in (39).) Now observe $(t, t_0) \mapsto D_2\varphi(t,x,v) D_2\varphi(t_0,x,v)^{-1}$ is the transition matrix of the homogeneous system associated with (40) and apply the solution formula for linear differential equations [54] to (40) to see that $\Phi'(x)^{-1}\Phi''(x)h^2$ equals the integral in (38) with t substituted for δ. Proposition IV.1 shows $\Phi(\Theta(s))$ is convex, and the theorem follows from Lemma A.2. □

Theorems IV.5 and IV.6 with the choice $t = N \cdot T$ provide sufficient conditions for attainable sets of the sampled system (1) to be convex, as required in hypothesis (H$_2$) of Section III. In the case of Theorem IV.5, that condition can be verified directly from properties of the right hand side F of the continuous-time system (2) by estimating

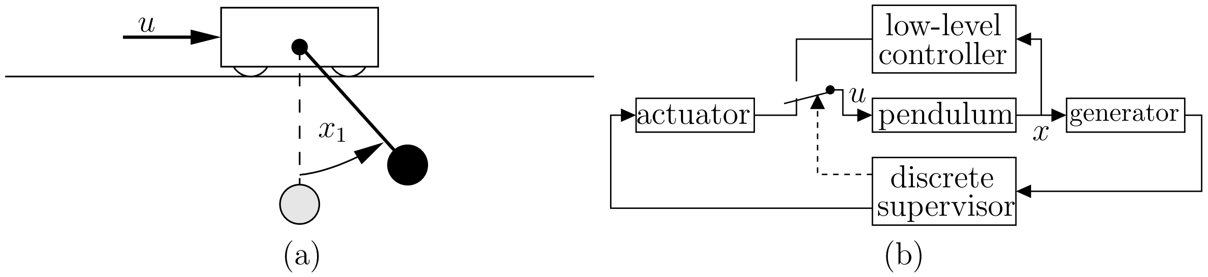


Figure 5. Example investigated in Section V: The pendulum (a) is swung up by the hybrid control system (b).

eigenvalues and a Lipschitz constant, with M_2 being just a bound on $\|D_1^2 F(x,w)\|$ if F is of class C^2 with respect to its first argument. In contrast, application of Theorem IV.6 requires estimating the integrand in (38). That higher effort often pays off when it results in larger bounds on r than (37). Note that, in view of the algorithm proposed in this paper, larger bounds will typically translate into lower computational complexity; see Fig. 4(b).

V. Example

In this section we shall demonstrate an application of our results from Sections III and IV within the framework of abstraction based supervisory control of sampled systems by solving a nonlinear, global problem with constraints. To begin with, consider the system

$$\dot{x}_1 = x_2, \tag{41a}$$

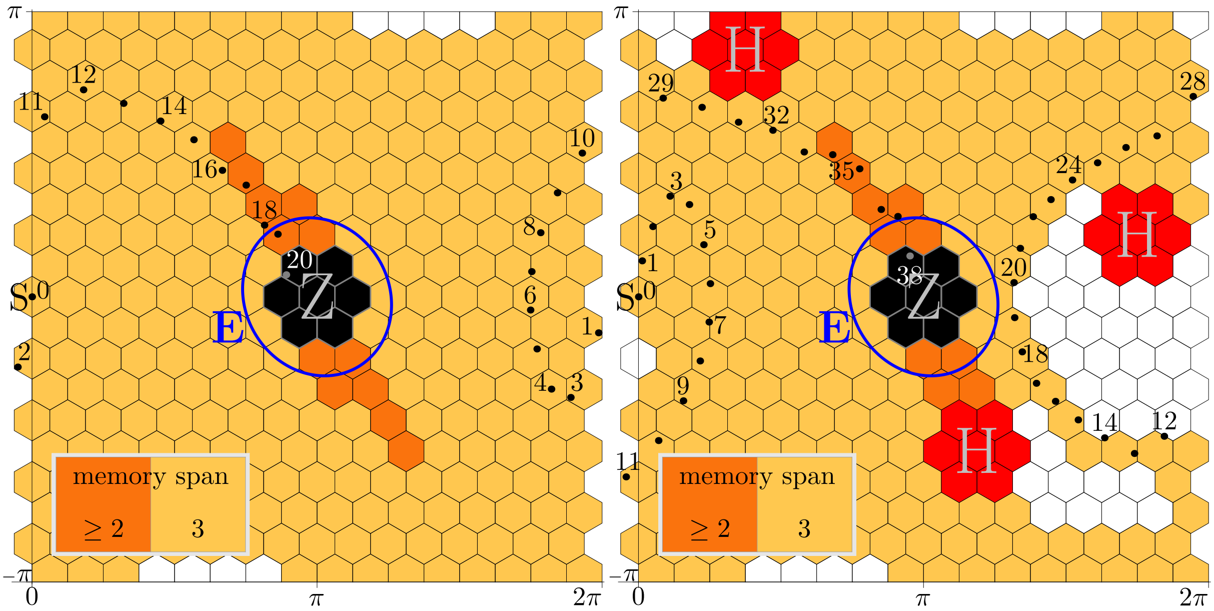
$$\dot{x}_2 = -\omega^2 \sin(x_1) - u\,\omega^2 \cos(x_1) - 2\gamma x_2, \tag{41b}$$

which describes the motion of a pendulum mounted on a cart. Here, ω and γ are parameters, specifically, γ is a friction coefficient, and x_1 is the angle between the pendulum and the downward vertical. See Fig. 5(a). The motion of the cart is not modeled; its acceleration u is considered a control.

We seek to swing up the pendulum by means of the hybrid control system shown in Fig. 5(b), which possesses a simple hierarchical structure. The low-level controller is to stabilize the pendulum at its upright position. That is, the point $(\pi, 0)$ becomes an asymptotically stable equilibrium of the closed loop composed of (41) and the low-level controller, so there will be some non-trivial, positively invariant subset E of its stability region. The supervisor, on the other hand, would force the state from some neighborhood of the origin into E and on success, would hand over control to the low-level controller. The supervisor will be realized by a finite automaton, which is why it is connected to the continuous plant via interface devices [3], to the effect that the open loop composed of actuator, pendulum and generator is represented by the sampled and quantized system (1),(3) associated with (41).

A suitable low-level controller together with a positively invariant set E is straightforward to determine [11], [60]. For example, if $\omega > 0$ and $0 \leq \gamma \leq \omega$, the affine state feedback $u = 2(\pi - x_1 - x_2/\omega)$ stabilizes (41) at $(\pi, 0)$, with the positively invariant ellipsoid

$$E = (\pi, 0) + \left\{ x \in \mathbb{R}^2 \,\middle|\, 63\omega^2 x_1^2 + 12\omega x_2 x_1 + 56 x_2^2 \leq 42\omega^2 \right\}$$



(a) (b)

Figure 6. (a) The state space of the pendulum system (41) is covered with quantizer cells. Supervisors designed on the basis of abstractions of memory span $N \in \{2, 3\}$ force the sampled and quantized pendulum system into the stability region E of the low-level controller, from anywhere in the indicated regions. The region for $N = 3$ contains the origin; one particular trajectory is shown. (b) Problem from (a) with extra constraints in the form of three obstacles in state space, which are labeled H in the illustration.

being a subset of the stability region. Here we focus on the design of quantizer and supervisor. So, let us consider a sampled version (1) of (41) and impose the constraints

$$|x_2| \leq \pi, \tag{42a}$$

$$|u| \leq 2, \tag{42b}$$

which model physical limits of an experimental setup. For the sake of simplicity, we choose controls to be constant on a common sampling interval $[0, T]$, specifically,

$$U = \{t \mapsto 0, t \mapsto -2, t \mapsto 2\}$$

in the notation of Section II-C. This guarantees the sampled system (1) fulfills hypothesis (H_1).

We next design a suitable quantizer (3) as part of the generator device in the hybrid control system of Fig. 5(b). To this end, assume that the control constraint (42b) is satisfied and that problem data and sampling period are given by

$$\omega = 1, \gamma = 0.01, T = 0.2.$$

Theorem A.4 in the Appendix shows that the attainable set $\varphi(t, \Omega, u)$ is convex whenever $\Omega \subseteq \mathbb{R}^2$ is r-convex, $r > 0.4$, and $0 \leq t \leq 3T = 0.6$, where φ denotes the general solution of (41). This implies any translated and possibly truncated copy of the regular hexagon given by its set

$$\frac{\pi}{16\sqrt{3}}\{(0, \pm 2), (\sqrt{3}, \pm 1), (-\sqrt{3}, \pm 1)\} \tag{43}$$

of vertices, which has circumradius $\pi/(8\sqrt{3}) < 0.23$, may be chosen as a quantizer cell in the computation of abstractions of memory span up to 3. Further, in view of the state

Table I
Computation of abstractions of the pendulum example.

N	half-spaces	polyhedra	states	transitions
1	7170	41059	306	4246
2	22914	97203	4552	35734
3	69048	351523	36040	220442

constraint (42a) we may restrict our investigation of the dynamics of (41) to the region K defined by $K = \mathbb{R} \times [-\pi, \pi]$. So, let us choose C' as a set of 304 translated copies of the hexagon (43), each intersected with K. This intersection either leaves a hexagon unchanged or results in an irregular pentagon; see Fig. 6. Finally, supplement C' with two overflow symbols,

$$C = C' \cup \{\mathbb{R} \times [\pi, \infty[\,, \mathbb{R} \times]-\infty, -\pi]\}.$$

Note that since the right hand side of (41) is periodic in x with period $(2\pi, 0)$, we have implicitly considered the system (41) on the cylinder [11], [54]. Having said this, C can really be regarded as a covering of the state space of (1).

With the choices we have made above, hypotheses (H_1) and (H_2) in Sections II and III are fulfilled. In particular, Theorem A.4 in the Appendix shows that for each cell $\Delta \in C'$, we may choose the smallest intersection of six closed balls of radius 0.4 containing Δ for the set $\widehat{\Delta}$ in hypothesis (H_2); see Fig. 2. We finally choose $\Sigma(\widehat{\Delta})$ to consist of six supporting half-spaces of $\widehat{\Delta}$ as in Fig. 2, and analogously for the pentagons in C'. The set $\Sigma(\widehat{\Delta})$ is then supplied to the algorithm in Fig. 3 to compute abstractions of the sampled and quantized pendulum system defined earlier. The results are summarized in Tab. I: The memory span N of the abstractions we have computed, the number of half-spaces determined from solutions of ODE (21), the number of polyhedra tested for emptiness, and the number of states and transitions in a finite automaton realization [43]–[45] of the abstraction. The data in Tab. I highlights the fact that half-spaces are shared among polyhedra, which is an important feature of the algorithm from Section III. Indeed, while each transition corresponds to a non-empty intersection of half-spaces, the number of those transitions by far exceeds the total number of computed half-spaces if $N > 1$.

In order to obtain a suitable supervisor for the control system of Fig. 5(b), we solve certain auxiliary control problems posed in terms of the abstractions already computed. So, let $N \in \{1, 2, 3\}$, denote by B_N the abstraction of memory span N that we have computed, define a start region S and a target region Z by

$$S = \{\Delta \in C' \,|\, (0,0) \in \Delta\}\,,$$
$$Z = \{\Delta \in C' \,|\, \Delta \subseteq E\}\,,$$

see Fig. 6, and consider the following problem: Determine the supervisor in the form of a map $R \colon \bigcup_{k=1}^{N} U^{k-1} \times C^k \to U$ such that whenever $(u, \Delta) \in B_N$, $\Delta_0 \in S$, and $u_k = R(u|_{]k-N;k[}, \Delta|_{]k-N;k]})$ for all $k \in \mathbb{Z}_+$, then there is some $k \in \mathbb{Z}_+$ such that $\Delta_k \in Z$ and $\Delta_\tau \in C'$ for all $\tau \in [0; k[$. This specification requires that if (u, Δ) is any signal that may possibly be produced by the closed loop composed of the supervisor R and some plant that realizes the behavior B_N, and if that signal additionally starts in S, then it remains in C' until it eventually enters Z. While its specification is not a complete behavior [43], that kind of discrete control problem is equivalent to a shortest path problem in some hypergraph [61], and thus, can be efficiently solved [62]. In fact, we have been able to

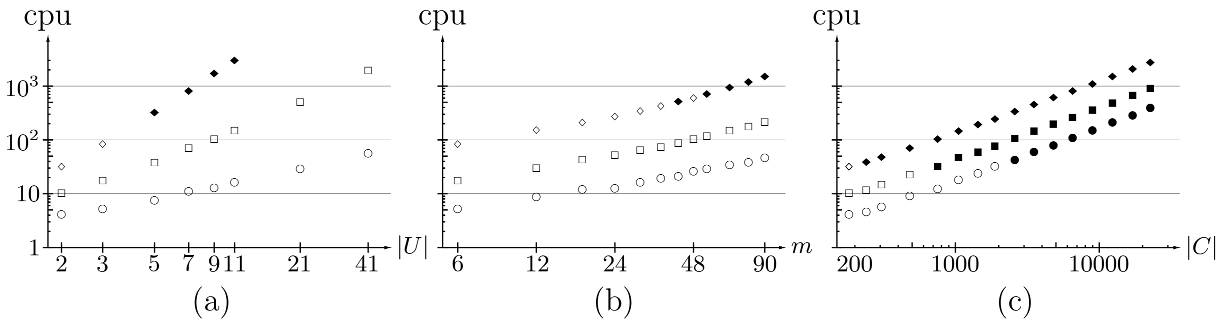


Figure 7. Dependence of run times in seconds on the number $|U|$ of controls, the number m of half-spaces supporting $\widehat{\Delta}$, and the number $|C|$ of quantizer cells, of an implementation of the algorithm in Fig. 3 with *Mathematica 7.0* [63], run on four threads of an Intel Xeon CPU E5620 (2.4 GHz). Results for memory spans 1, 2 and 3 correspond to the symbols ∘, □, and ◊, respectively, which are filled iff the corresponding abstraction has lead to a solution of the control problem considered in Section V. (a) $|C| = 182$, $m = 6$. (b) $|U| = 3$, $|C| = 182$. (c) $|U| = 2$, $m = 6$.

obtain a supervisor R in the case $N = 3$, and to prove there is none enforcing the above specification if $N \in \{1, 2\}$, with run times negligible compared to the ones observed in the computation of the abstractions. Specifically, for $N = 3$, the target region is reached within at most 27 steps. It follows that R is compatible with the actual plant, i.e., with the sampled and quantized pendulum system defined earlier, and also enforces the above specification when combined with that plant rather than with the abstraction B_3, on which the design of R was based [46]. See also Fig. 6(a).

Modifying the above example, we have varied the number of controls, the number of supporting hyperplanes, and the number of quantizer cells. See Fig. 7. Given the fact that the reported run times have been obtained from interpreted rather than from compiled code, we expect that the algorithm in Fig. 3 can also be successfully applied to systems essentially more complex than (41). See also [64]. Fig. 7(b) also demonstrates the importance of accurately approximating attainable sets. In particular, we have verified for the quantizer used in Fig. 7(b) that the control problem considered in this section could not be solved using ellipsoidal rather than strongly convex supersets of quantizer cells.

We have additionally investigated a scenario with extra constraints in the form of obstacles in state space, by simply treating the obstacle cells as overflow symbols. The results illustrated in Fig. 6(b) show that our approach would also be feasible in the presence of complicated constraints such as the ones regularly met in motion planning problems [12].

Finally, we would like to point out that the supervisors we have designed solve control problems for a sampled version of (41). In fact, the discrete abstractions we are using are not capable of representing the evolution of continuous-time systems between sampling times, and hence, control problems for the latter systems cannot be treated directly. However, solutions for an important class of continuous-time control problems can be obtained from solutions of auxiliary problems for sampled systems using a robust version of the original specification, e.g. [65]. For the problem considered in this section, a robust specification could easily be obtained by tightening state constraints, i.e., by decreasing the bound (42a) and enlarging the obstacles in Fig. 6(b) by a suitable amount.

VI. Conclusions

We have presented a novel algorithm for the computation of discrete abstractions of nonlinear systems as well as a set of sufficient conditions for the convexity of attainable sets. While the usefulness of the first relies on the second contribution, the latter may be of separate interest. Practicability of our results in the design of discrete controllers for nonlinear continuous plants under state and control constraints has been demonstrated by an example, and we also expect their use to be of advantage in attainability and verification problems.

The algorithm proposed in this paper is the first one that not only yields abstractions of finite but otherwise arbitrary memory span that are suitable for solving general control problems, but also applies to nonlinear systems under rather mild conditions, which essentially reduce to sufficient smoothness in the case of sampled systems. Previous approaches are confined to abstractions of memory span 1 with two exceptions, which apply only to monotone dynamics [28] and are not rigorous and limited to solving reachability problems [39], respectively. We emphasize that increasing the memory span may be the only way to improve the accuracy of abstractions up to a level at which analysis and synthesis problems can be solved. One example is networked control systems [13], where quantization effects are part of the systems to be investigated and state space quantizations cannot be arbitrarily refined.

Its wide applicability and the fact that it builds on relatively simple computations distinguishes our approach from competing techniques even if we restrict ourselves to abstractions of memory span 1. In particular, some methods only apply to systems whose continuous-valued dynamics is defined by ordinary difference and differential equations with multi-affine or polynomial right hand sides [29]–[31], or require stability [26], [27] or deriving a state space partition in accordance with the exact system dynamics prior to their application [40]–[42]. Others require the use of interval arithmetic [32]–[35], deciding satisfiability of formulas over certain logical theories [36], or solving complex optimization problems [23], [37], [38].

Finally, a distinctive feature of our method is that the error by which attainable sets of quantizer cells are over-approximated is quadratic in the size of the cells. This has been achieved by extending our earlier results from [47], [48] to apply to strongly convex sets rather than merely ellipsoids. Due to this improvement, our method will outperform the sampling method [25] and any other method whose approximation error depends linearly on the dispersion [12] of some grid, e.g. [26], [27], [50], whenever highly accurate abstractions are to be computed.

The techniques we propose can currently be applied to systems with finite input alphabets only and additionally depend on the ability to design suitable quantizers. The latter can be quite demanding, despite the results presented here. An extension to systems with continuous inputs and an automated procedure for designing quantizers would considerably enhance our method. It should also be extended to account for disturbances and uncertainties, including numerical discretization errors and the effects of finite arithmetic in order to address robustness issues and to obtain validated results.

Acknowledgment

The author thanks B. Farrell (München) and O. Stursberg (Kassel) for their valuable comments on earlier versions of this paper, as well as A. Herrmann (Berlin), for providing convenient access to computing facilities.

Appendix

A.1 Lemma. *Let $r > 0$, $z \in \mathbb{R}^n$, $x, y \in \bar{B}(z, r)$, $x \neq y$, and $s = \|x - y\|^2/(8r)$. Then $\bar{B}((x+y)/2, s) \subseteq \bar{B}(z, r)$.*

Proof. Let A be an arc of a circle of radius r joining x and y whose length does not exceed πr. Then $A \subseteq \bar{B}(z, r)$, e.g. [55], and $\min \{\|a - (x+y)/2\| \mid a \in A\} = r - (r^2 - \|x - y\|^2/4)^{1/2}$. The latter is easily shown to be bounded below by s. □

The *Hausdorff distance* between any non-empty, compact subsets $M, N \subseteq \mathbb{R}^n$ is defined to be the infimum of $r \in \mathbb{R}_+$ for which both $M \subseteq N + \bar{B}(0, r)$ and $N \subseteq M + \bar{B}(0, r)$ [59].

A.2 Lemma. *Let $M \subseteq \mathbb{R}^n$, $M \neq \emptyset$, and define $\Theta(s) = \bigcap_{x \in M} \bar{B}(x, s)$ for all $s > 0$. If $r > 0$ and $\Theta(r)$ contains at least two points, then $\lim_{s \to r, s < r} \Theta(s) = \Theta(r)$ in Hausdorff distance.*

Proof. $\Theta(s)$ is convex and compact for any $s > 0$, and $\Theta(r)$ possesses nonempty interior by Lemma A.1; hence $\Theta(r) = \operatorname{cl}(\operatorname{int}(\Theta(r)))$. If $p \in \operatorname{int} \Theta(r)$, then $p \in \Theta(s)$ whenever s is sufficiently close to r, in particular, $\Theta(s) \neq \emptyset$. Thus the Hausdorff distance between $\Theta(s)$ and $\Theta(r)$ is well-defined. Moreover, given $\varepsilon > 0$ and $y \in \Theta(r)$, there is $p \in \operatorname{int} \Theta(r)$ with $\|p - y\| < \varepsilon$, hence $y \in \Theta(s) + B(0, \varepsilon)$ for some $s < r$, where $B(x, r)$ denotes the open Euclidean ball of radius r centered at x. This shows $\Theta(r) \subseteq \bigcup_{s \in]0, r[} (\Theta(s) + B(0, \varepsilon))$, and compactness of $\Theta(r)$ implies $\Theta(r) \subseteq \Theta(s) + B(0, \varepsilon)$ for some $s < r$, hence for all $s < r$ sufficiently close to r. □

A.3 Lemma. *Let $P_1, \dots, P_k \subseteq \mathbb{R}^n$ be convex polyhedra. Then $\operatorname{cl}(\mathbb{R}^n \setminus \bigcup_{i=1}^k P_i)$ is the finite union of convex polyhedra.*

Proof. For any polyhedron $M = \{x \in \mathbb{R}^n \mid Ax \leq b\}$, A an $m \times n$-matrix, $b \in \mathbb{R}^m$, $m \geq 1$, the closure of $\mathbb{R}^n \setminus M$ equals $\bigcup_{j=1}^m \{x \in \mathbb{R}^n \mid A_j x \geq b_j\}$, where A_j denotes the jth row of A. Therefore, $\operatorname{cl}\left(\mathbb{R}^n \setminus \bigcup_{i=1}^k P_i\right) = \bigcap_{i=1}^k \operatorname{cl}(\mathbb{R}^n \setminus P_i) = \bigcap_{i=1}^k \bigcup_{j=1}^m Q_{i,j}$ for suitable half-spaces $Q_{i,j}$. Since intersection and union distribute over each other, the right hand side of the previous identity equals $\bigcup_{j \in J^I} \bigcap_{i \in I} Q_{i,j_i}$, where $I = [1; k]$ and $J = [1; m]$. □

A.4 Theorem. *Let $t > 0$ and assume the input u to the pendulum equations (41) is piecewise continuous with $|u(\tau)| \leq \hat{u}$ for all $\tau \in [0, t]$. Define*

$$\widehat{\omega} = \max \left\{ 1, |\omega| \left(1 + \hat{u}^2\right)^{1/4} \right\},$$

$$r = \frac{12 \widehat{\omega}^2 \, (1 + (\widehat{\omega} + \gamma)^2)^{-3/2}}{\sinh(3\widehat{\omega} t) + \sinh(\widehat{\omega} t) \, (12(\widehat{\omega}^{-2} + 1)^{-3/2} - 3)},$$

where max *denotes the maximum, and assume $0 \leq \gamma \leq \frac{3}{4}\widehat{\omega}$ and $2(\widehat{\omega}^2 - \gamma^2)^{1/2} t \leq \pi$. Then the attainable set $\varphi(t, \Omega, u)$ is convex for any r-convex subset $\Omega \subseteq \mathbb{R}^2$, where φ denotes the general solution of (41).*

Proof. First note that the right hand side of (41) is linearly bounded [54], which implies $\varphi(\tau, \mathbb{R}^2, u) = \mathbb{R}^2$ for any $\tau \in \mathbb{R}_+$. One may therefore assume $\Omega \neq \mathbb{R}^2$ without loss of generality. Then apply Theorem IV.6 and use the estimate

$$\omega^2 |u(\tau) \cos(\varphi(\tau, x_0, u)_1) + \sin(\varphi(\tau, x_0, u)_1)| \leq \widehat{\omega}^2,$$

the fact that $D_2\varphi(\cdot,x,u)$ fulfills the variational equation to (41) along $\varphi(\cdot,x,u)$, Cramer's rule, and the formula of Abel–Liouville [54] to see that it suffices to show

$$\widehat{\omega}^2 \int_0^t \mathrm{e}^{2\gamma\tau} \, \|(D_2\varphi(\tau,x_0,u))_{1,\cdot}\|^3 \, d\tau \leq 1/r. \tag{44}$$

Here, the subscript "$1,\cdot$" denotes the first row. Now set $\kappa = (\widehat{\omega}^2+\gamma^2)^{1/2}$ and observe $(1+(\kappa+\gamma)^2)\,\kappa^{-2} \leq (1+(\widehat{\omega}+\gamma)^2)\,\widehat{\omega}^{-2}$ to obtain the upper bound

$$\frac{\mathrm{e}^{-2\gamma\tau}}{2\widehat{\omega}^2}(1+(\widehat{\omega}+\gamma)^2)\left(\cosh(2\kappa\tau)+\frac{\widehat{\omega}^2-1}{\widehat{\omega}^2+1}\right) \tag{45}$$

for the squared norm of the first row of $\exp\left(\tau\left(\begin{smallmatrix}0 & 1\\ \widehat{\omega}^2 & -2\gamma\end{smallmatrix}\right)\right)$. The second step of the proof of [47, Theorem 6] shows (45) is also an upper bound for $\|(D_2\varphi(\tau,x_0,u))_{1,\cdot}\|^2$. Next show

$$h(\alpha) := \frac{\cosh\left((9\beta^2+(\alpha+4\beta)^2)^{1/2}\right)}{\cosh(\alpha+4\beta)} - \mathrm{e}^{\beta} \leq 0 \tag{46}$$

for all $\alpha,\beta \geq 0$. The choice $\alpha = 2(\widehat{\omega}-4\gamma/3)\tau$, $\beta = 2\gamma\tau/3$ then yields the upper bound

$$\frac{\mathrm{e}^{-4\gamma\tau/3}}{\widehat{\omega}^2}(1+(\widehat{\omega}+\gamma)^2)\left(\cosh(\widehat{\omega}\tau)^2-\frac{1}{\widehat{\omega}^2+1}\right) \tag{47}$$

for $\|(D_2\varphi(\tau,x_0,u))_{1,\cdot}\|^2$. Indeed, the map h defined in (46) is continuous, and for every $\alpha > 0$, $h'(\alpha)$ exists and is a positive multiple of

$$\tanh(\mu+\nu)/\tanh(\mu) - (\mu+\nu)/\mu, \tag{48}$$

where $\mu = \alpha+4\beta$ and $\nu = (9\beta^2+\mu^2)^{1/2}-\mu$. (48) is monotonically decreasing with respect to $\nu \geq 0$ and vanishes for $\nu = 0$. Thus h is monotonically decreasing on $\mathbb{R}_+$. This proves (46) since $h(0) \leq 0$.

Finally, consider the map g defined on $[0,1]$ by

$$g(s) = 1 - s\left(1-\frac{\widehat{\omega}^3}{(\widehat{\omega}^2+1)^{3/2}}\right) - \left(1-\frac{s}{\widehat{\omega}^2+1}\right)^{3/2}.$$

This map is concave since $g''(s) < 0$, and $g(0) = g(1) = 0$; thus g is non-negative. For the choice $s = \cosh(\widehat{\omega}\tau)^{-2}$, this together with the bound (47) implies $\|D_2\varphi(\tau,x_0,u)_{1,\cdot}\|^3$ does not exceed

$$\mathrm{e}^{-2\gamma\tau}\widehat{\omega}^{-3}(1+(\widehat{\omega}+\gamma)^2)^{3/2}\left(\cosh(\widehat{\omega}\tau)^3-\cosh(\widehat{\omega}\tau)\left(1-\widehat{\omega}^3(\widehat{\omega}^2+1)^{-3/2}\right)\right),$$

which directly implies (44). □

References

[1] C. S. Hsu, *Cell-to-cell mapping*, Applied Mathematical Sciences. New York: Springer-Verlag, 1987, vol. 64.

[2] R. Alur, T. A. Henzinger, G. Lafferriere, and G. J. Pappas, "Discrete abstractions of hybrid systems," *Proc. IEEE*, vol. 88, no. 7, pp. 971–984, Jul. 2000.

[3] X. D. Koutsoukos, P. J. Antsaklis, J. A. Stiver, and M. D. Lemmon, "Supervisory control of hybrid systems," *Proc. IEEE*, vol. 88, no. 7, pp. 1026–1049, Jul. 2000.

[4] M. Dellnitz and O. Junge, "Set oriented numerical methods for dynamical systems," in *Handbook of dynamical systems*, B. Fiedler, Ed. Amsterdam: North-Holland, 2002, vol. 2, pp. 221–264.

[5] J. Ding, T. Y. Li, and A. Zhou, "Finite approximations of Markov operators," *J. Comput. Appl. Math.*, vol. 147, no. 1, pp. 137–152, 2002.

[6] J. Schröder, *Modelling, state observation and diagnosis of quantised systems*, Lect. Notes Control Inform. Sciences. Berlin: Springer-Verlag, 2003, vol. 282.

[7] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and fault-tolerant control.* Berlin: Springer, 2006.

[8] G. Osipenko, *Dynamical systems, graphs, and algorithms*, Lecture Notes in Mathematics. Berlin: Springer-Verlag, 2007, vol. 1889.

[9] P. Tabuada, *Verification and control of hybrid systems.* Springer, 2009.

[10] C. Tomlin, G. J. Pappas, and S. Sastry, "Conflict resolution for air traffic management: a study in multiagent hybrid systems," *IEEE Trans. Automat. Control*, vol. 43, no. 4, pp. 509–521, 1998.

[11] E. D. Sontag, *Mathematical control theory*, 2nd ed., Texts in Applied Mathematics. Springer, 1998, vol. 6.

[12] S. M. LaValle, *Planning algorithms.* Cambridge University Press, 2006.

[13] A. S. Matveev and A. V. Savkin, *Estimation and control over communication networks*, Control Engineering. Birkhäuser Boston, 2009.

[14] R. Kumar and V. K. Garg, *Modeling and control of logical discrete event systems.* Kluwer, 1995.

[15] E. M. Clarke, O. Grumberg, and D. A. Peled, *Model Checking.* MIT Press, 1999.

[16] C. G. Cassandras and S. Lafortune, *Introduction to discrete event systems*, 2nd ed. New York: Springer, 2008.

[17] D. Lind and B. Marcus, *An introduction to symbolic dynamics and coding.* Cambridge University Press, 1995.

[18] S. H. Crandall, K. L. Chandiramani, and R. G. Cook, "Some first passage problems in random vibration," *Journal of Applied Mechanics, ASME*, vol. 33, pp. 532–538, 1966.

[19] P. K. C. Wang, "A method for approximating dynamical processes by finite-state systems," *Int. J. Control, I.* , vol. 8, pp. 285–296, 1968.

[20] C. S. Hsu, R. S. Guttalu, and W. H. Zhu, "A method of analyzing generalized cell mappings," *Trans. ASME Ser. E J. Appl. Mech.*, vol. 49, no. 4, pp. 885–894, 1982.

[21] L. Grüne, *Asymptotic behavior of dynamical and control systems under perturbation and discretization*, Lecture Notes in Mathematics. Berlin: Springer-Verlag, 2002, vol. 1783.

[22] C. S. Hsu, "Domain-to-domain evolution by cell mapping," in *Nonlinear dynamics and stochastic mechanics*, CRC Math. Model. Ser. Boca Raton, FL: CRC, 1995, pp. 45–68.

[23] L. Grüne and O. Junge, "Approximately optimal nonlinear stabilization with preservation of the Lyapunov function property," in *Proc. 46th IEEE Conf. Decision and Control (CDC), New Orleans, Louisiana, U.S.A., 2007.* New York: IEEE, 2007, pp. 702–707.

[24] C. S. Hsu, "A discrete method of optimal control based upon the cell state space concept," *J. Optim. Th. Appl.*, vol. 46, no. 4, pp. 547–569, 1985.

[25] O. Junge, "Rigorous discretization of subdivision techniques," in *International Conference on Differential Equations (Berlin, 1999).* World Sci. Publ., River Edge, NJ, 2000, pp. 916–918.

[26] P. Tabuada, "An approximate simulation approach to symbolic control," *IEEE Trans. Automat. Control*, vol. 53, no. 6, pp. 1406–1418, 2008.

[27] G. Pola and P. Tabuada, "Symbolic models for nonlinear control systems: alternating approximate bisimulations," *SIAM J. Control Optim.*, vol. 48, no. 2, pp. 719–733, 2009.

[28] T. Moor and J. Raisch, "Abstraction based supervisory controller synthesis for high order monotone continuous systems," in *Modelling, Analysis, and Design of Hybrid Systems*, Lect. Notes Control Inform. Sciences, S. Engell, G. Frehse, and E. Schnieder, Eds. Springer, 2002, vol. 279, pp. 247–265.

[29] O. Maler and G. Batt, "Approximating continuous systems by timed automata," in *Formal methods in systems biology*, Lect. Notes Computer Science. Berlin: Springer, 2008, vol. 5054, pp. 77–89.

[30] S. Berman, Á. Halász, and V. Kumar, "MARCO: A reachability algorithm for multi-affine systems with applications to biological systems," in *Proc. 10th Intl. Conf. Hybrid Systems: Computation and Control (HSCC), Pisa, Italy, Apr. 3-5, 2007*, Lect. Notes Computer Science, A. Bemporad, A. Bicchi, and G. Buttazzo, Eds., vol. 4416. Springer, 2007, pp. 76–89.

[31] A. Girard and G. J. Pappas, "Approximate bisimulations for nonlinear dynamical systems," in *Proc. 44th IEEE Conf. Decision and Control, and the Europ. Control Conf., Seville, Spain, Dec. 12-15, 2005.* IEEE, 2005, pp. 684–689.

[32] L. Jaulin and E. Walter, "Global numerical approach to nonlinear discrete-time control," *IEEE Trans. Automat. Control*, vol. 42, no. 6, pp. 872–875, 1997.

[33] O. Stursberg, S. Kowalewski, and S. Engell, "On the generation of timed discrete approximations for continuous systems," *Math. Comput. Model. Dyn. Syst.*, vol. 6, no. 1, pp. 51–70, 2000.

[34] M. Althoff, O. Stursberg, and M. Buss, "Computing reachable sets of hybrid systems using a combination of zonotopes and polytopes," *Nonlinear Anal. Hybrid Syst.*, vol. 4, no. 2, pp. 233–249, 2010.

[35] Y. Tazaki and J. Imura, "Discrete-state abstractions of nonlinear systems using multi-resolution quantizer," in *Proc. 12th Intl. Conf. Hybrid Systems: Computation and Control (HSCC), San Francisco, U.S.A., Apr. 13-15, 2009*, Lect. Notes Computer Science, R. Majumdar and P. Tabuada, Eds., vol. 5469. Springer, 2009, pp. 351–365.

[36] A. Tiwari, "Abstractions for hybrid systems," *Form. Methods Syst. Des.*, vol. 32, no. 1, pp. 57–83, Feb. 2008.

[37] A. Chutinan and B. H. Krogh, "Computational techniques for hybrid system verification," *IEEE Trans. Automat. Control*, vol. 48, no. 1, pp. 64–75, 2003.

[38] I. M. Mitchell, A. M. Bayen, and C. J. Tomlin, “A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamic games,” *IEEE Trans. Automat. Control*, vol. 50, no. 7, pp. 947–957, 2005.

[39] L. Grüne and F. Müller, “Set oriented optimal control using past information,” in *Proc. 2008 Math. Th. of Networks and Systems (MTNS), Blacksburg, Virginia, U.S.A., Jul. 28-Aug. 1*, 2008.

[40] M. Broucke, “A geometric approach to bisimulation and verification of hybrid systems,” in *Proc. 37th IEEE Conf. Decision and Control (CDC), Tampa, Florida, USA*. IEEE, Dec. 1998, pp. 4277–4282.

[41] P. E. Caines and Y.-J. Wei, “Hierarchical hybrid control systems: a lattice-theoretic formulation,” *IEEE Trans. Automat. Control*, vol. 43, no. 4, pp. 501–508, 1998.

[42] J. A. Stiver, X. D. Koutsoukos, and P. J. Antsaklis, “An invariant-based approach to the design of hybrid control systems,” *Internat. J. Robust Nonlinear Control*, vol. 11, no. 5, pp. 453–478, 2001.

[43] J. C. Willems, “Models for dynamics,” in *Dynamics reported, Vol. 2*, Dynam. Report. Ser. Dynam. Systems Appl. Chichester: Wiley, 1989, vol. 2, pp. 171–269.

[44] T. Moor, “Approximationsbasierter Entwurf diskreter Steuerungen für gemischtwertige Regelstrecken,” Dissertation, Univ. der Bundeswehr, Hamburg, Fachbereich Elektrotechnik, Hamburg, Germany, 1999.

[45] T. Moor and J. Raisch, “Supervisory control of hybrid systems within a behavioural framework,” *Systems Control Lett.*, vol. 38, no. 3, pp. 157–166, 1999.

[46] T. Moor, J. M. Davoren, and B. D. O. Anderson, “Robust hybrid control from a behavioural perspective,” in *Proc. 41th IEEE Conference on Decision and Control, Las Vegas, U.S.A., 2002*. New York: IEEE, 2002, pp. 1169–1174.

[47] G. Reißig, “Convexity of reachable sets of nonlinear ordinary differential equations,” *Automat. Remote Control*, vol. 68, no. 9, pp. 1527–1543, Sep. 2007, http://www.reiszig.de/gunther/pubs/i07Convex.abs.html

[48] ——, “Convexity of reachable sets of nonlinear discrete-time systems,” in *Proc. 13th IEEE Int. Conf. Methods and Models in Automation and Robotics (MMAR), Szczecin, Poland, Aug. 27-30, 2007*, R. Kaszyński, Ed., 2007, pp. 199–204.

[49] F. A. Valentine, *Convex sets*. New York: McGraw-Hill, 1964.

[50] G. Reißig, “Computation of discrete abstractions of arbitrary memory span for nonlinear sampled systems,” in *Proc. 12th Intl. Conf. Hybrid Systems: Computation and Control (HSCC), San Francisco, U.S.A., Apr. 13-15, 2009*, Lect. Notes Computer Science, R. Majumdar and P. Tabuada, Eds., vol. 5469. Springer, 2009, pp. 306–320.

[51] E. Schechter, *Handbook of analysis and its foundations*. San Diego, CA: Academic Press Inc., 1997.

[52] G. Reißig, “Local fill reduction techniques for sparse symmetric linear systems,” *Arch. Elektrotech.*, vol. 89, no. 8, pp. 639–652, Sep. 2007, avail. at http://www.reiszig.de/gunther/pubs/i06Fill.abs.html

[53] P. M. Gruber, *Convex and discrete geometry*, Fundamental Principles of Mathematical Sciences. Berlin: Springer, 2007, vol. 336.

[54] P. Hartman, *Ordinary differential equations*, Classics in Applied Mathematics. Philadelphia, PA, U.S.A.: SIAM, 2002, vol. 38.

[55] H. Frankowska and C. Olech, “R-convexity of the integral of set-valued functions,” in *Contributions to analysis and geometry (Baltimore, Md., U.S.A., 1980, Suppl. Amer. J. Math.)*. Baltimore, Md., U.S.A: Johns Hopkins Univ. Press, 1981, pp. 117–129.

[56] E. S. Polovinkin, “Strongly convex analysis,” *Mat. Sb.*, vol. 187, no. 2, pp. 103–130, 1996, (Russian. Engl. transl. in Russian Acad. Sci. Sb. Math., vol. 187, 1996, no. 2, 259–286).

[57] D. Bednařík and K. Pastor, “Elimination of strict convergence in optimization,” *SIAM J. Control Optim.*, vol. 43, no. 3, pp. 1063–1077, 2004.

[58] V. Lakshmikantham and D. Trigiante, *Theory of difference equations: numerical methods and applications*, 2nd ed., Monographs and Textbooks in Pure and Applied Mathematics. New York: Marcel Dekker Inc., 2002, vol. 251.

[59] R. Webster, *Convexity*. New York: Oxford University Press, 1994.

[60] D. Henrion and A. Garulli, Eds., *Positive polynomials in control*, Lecture Notes in Control and Information Sciences. Berlin: Springer-Verlag, 2005, vol. 312.

[61] C. M. Özveren, A. S. Willsky, and P. J. Antsaklis, “Stability and stabilizability of discrete event dynamic systems,” *J. Assoc. Comput. Mach.*, vol. 38, no. 3, pp. 730–752, 1991.

[62] G. Gallo, G. Longo, S. Pallottino, and S. Nguyen, “Directed hypergraphs and applications,” *Discrete Appl. Math.*, vol. 42, no. 2-3, pp. 177–201, 1993.

[63] S. Wolfram, *The Mathematica® book*, 5th ed. Wolfram Media, Inc., Champaign, IL, U.S.A., 2003.

[64] G. Reißig, “Abstraction based solution of complex attainability problems for decomposable continuous plants,” in *Proc. 49th IEEE Conf. Decision and Control (CDC), Atlanta, GA, U.S.A., 15-17 Dec. 2010*. New York: IEEE, 2010, pp. 5911–5917, avail. at http://www.reiszig.de/gunther/pubs/i10product.abs.html

[65] G. E. Fainekos, A. Girard, H. Kress-Gazit, and G. J. Pappas, “Temporal logic motion planning for dynamic robots,” *Automatica J. IFAC*, vol. 45, no. 2, pp. 343–352, 2009.